FiMM

7 August 2013

CIRCULAR : **LSRA/AL/AZ-ck/037-13**
(TOTAL NO. OF PAGE(S): 4)

TO :
i. MEMBERS, IUTA AND CUTA
ii. PRS PROVIDERS, INSTITUTIONAL PRS ADVISERS AND CORPORATE PRS ADVISERS

ATTN. : **AUTHORISED REPRESENTATIVE/CHIEF EXECUTIVE OFFICER**

FiMM'S GUIDANCE NOTE IN RELATION TO THE PERSONAL DATA PROTECTION ACT 2010

We refer to the above matter.

In line with the introduction of Personal Data Protection Act 2010 ("PDPA"), FIMM has been requested to provide its Members and Registered Persons with guidance note outlining the minimum measures that will need to be put into place in order to be compliant with the PDPA upon it coming into effect.

The PDPA provides protection and control on the collection, storing and usage of personal data by organizations that process such data for commercial transactions.

A copy of the abovementioned Guidance Note is enclosed for your attention and further action. A soft copy of the same may be made available on our website in due course.

Should you have any query, please contact Poh Khie Yee (Ext 300) or Sharon Kaur (Ext 309) of Legal, Secretarial & Regulatory Affairs at 03-2093 2600.

Thank you.

Yours faithfully,
Federation of Investment Managers Malaysia

AHMAD ZAKIE HJ. AHMAD SHARIFF
Chief Executive Officer

Encls.

FEDERATION OF INVESTMENT MANAGERS MALAYSIA (272577-P)
(formerly known as Federation of Malaysian Unit Trust Managers)
19-07-3, 7th Floor PNB Damansara, No.19 Lorong Dungun, 50490 Kuala Lumpur
• **T** 603 2093 2600 • **F** 603 2093 2700 • www.fimm.com.my

FIMM GUIDANCE NOTE IN RELATION TO THE PERSONAL DATA PROTECTION ACT 2010

A. BACKGROUND TO THE NOTE

In June 2010, the Parliament of Malaysia passed the **Personal Data Protection Act 2010 [Act 709]** ("PDPA") with the aim of regulating the collection, storage, processing and use of any personal data. While the PDPA has been passed by Parliament, the same has not come into effect. However, based on inquiries with the Jabatan Perlindungan Data Peribadi, FIMM has been informed that the PDPA is expected to come into effect any time from the mid of August 2013.

Due to the imminent enforcement of the PDPA, FIMM has been requested to provide its regulatees with a guideline outlining the minimum measures that will need to be taken in order to be compliant with the PDPA upon it coming into effect.

B. THE PDPA

The PDPA is not intended to obstruct the legitimate use of personal data but strives to ensure that it is used fairly. It aims to provide protection and control over the way ***personal data***[1]is collected, stored and used. It sets the standards which must be satisfied by an organization when ***processing***[2]such data in respect of ***commercial transactions***[3].

Organizations will be required to register with the Personal Data Protection Commission once the PDPA has been put into effect[4].

Under the PDPA, organizations processing personal data must comply with the following principles[5]: (i) General Principle; (ii) Notice and Choice Principle; (iii) Disclosure Principle; (iv) Security Principle; (v) Retention Principle; (vi) Data Integrity Principle; and (vii) Access Principle.

Failure to abide by any of the above principles amounts to an offence. Upon conviction, an organization will be liable to a fine not exceeding RM300,000 or to imprisonment of their relevant officers for a term not exceeding 2 years or to both[6].

The PDPA applies to both new and existing ***data subjects***[7]. In relation to existing data subjects[8], organizations will have a 3 month grace period to comply with the PDPA principles.

---

[1]Defined as any information that directly or indirectly relates to a ***data subject*** (i.e. individual) who is identified or identifiable from that information.
[2]Means any collection, recording, holding or storing of personal data which includes any organisation, adaption, alteration, retrieval, consultation, use , disclosure, correction, erasure, or destruction of personal data.
[3]Means any transaction of a commercial nature, irrespective of whether it is contractual or not, and includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance
[4]Processing personal data without registration will amount to an offence under S. 16(4) of the PDPA, and on conviction will be liable to a fine not exceeding RM500,000 or to imprisonment for a term not exceeding 3 years or to both.
[5]Pursuant to S. 7 of the PDPA
[6]Pursuant to S. 5(2) of the PDPA
[7]Means individuals who are the subject of personal data, i.e. employees, customers, agents, members of the public, etc..
[8]i.e. current and past customers, employees and business associates.

C. MINIMUM RECOMMENDED MEASURES

1. Provide A Privacy Notice[9]

Organizations are required to provide an adequate privacy notice to all data subjects in respect of whom personal data is collected and processed. The privacy notice will need to inform data subjects of the fact that (i) their personal data will be processed and used, (ii) the purpose of such processing and use, (iii) the source of the personal data, (iv) their right to request access to and correction of personal data, (v) possible third parties to whom such data will be disclosed, (vi) the choice that data subjects have as to the extent of information supplied, (vii) if the supply of such information is mandatory or optional, and (viii) where the supply of information is mandatory, the consequences should there be a failure to supply the same.

The privacy notice provided must be in writing and in the Malay and English languages. Privacy notices should be issued when personal data is first requested from the data subject or first collected by the organization.

The mode of communication of a privacy notice may, for the moment, be determined by the organization (e.g. website notice, direct mailers, notice in premises, etc.). However, please note that this is subject to the issuance of the PDPA Regulations and/or guidance by the Commissioner which may specify the manner in which a privacy notice should be communicated and accepted by data subjects.

2. Amend Forms & Related Terms and Conditions

The PDPA imposes an obligation on organizations to seek a data subjects' consent prior to collecting, using or disclosing the data subjects' personal data. As a matter of best practice, consent should be obtained in writing. The said consent should ideally be reflected in the organizations' application forms and in their related terms and conditions[10].

It is also recommended that standard forms used by organizations are re-examined and modified in order to be in-line with the PDPA. Principally, organizations are advised to indicate in the forms as to which information being requested is mandatory[11] and which information requested is optional. In order to arrive at a position on this matter, organizations need to be clear as to which information is absolutely required for transactional, reporting and regulatory purposes, and that which is not, i.e. optional information.

3. Amend Contracts

All contracts applicable to an organization's customers, employees and third party data processors[12] should be re-examined and amended where necessary to be in-line with the PDPA requirements. Particularly:-

(i) Contracts with customers should include provisions (a)referencing the organizations' privacy notice, acknowledging that the customer has read and understood the contents of the said notice, (b) consenting to the collection and processing of their personal data, and (iii) authorising disclosure to third parties as identified in the privacy notice.

---

[9] Pursuant to S.7 of the PDPA

[10] See no. 3 below.

[11] Where information being requested is mandatory, organizations are advised to inform data subjects in the privacy notice of the consequences of not providing such information.

[12] Means any person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purpose, e.g. IT outsourcers, printing and mailing vendors, security service providers, etc..

(ii) Contracts with employees[13] should include provisions (a) consenting to the access, collection and processing of their personal data, (b) authorising disclosure to third parties (e.g. to FIMM), and (c) requiring adherence to security and confidentiality policies where employees are involved in the processing of personal data of data subjects.

(iii) Contracts with data processors should include provisions (a) providing sufficient guarantees from the data processor relating to its "technical" and "organizational" security measures undertaken to protect the personal data supplied by the organization,and (b) authorizing the organization to take reasonable steps to check that those security measures are being put into practice.

4. Revise Existing Policies & Processes

Organizations may need to re-examine and revise existing policies and processes to ensure that the principles and requirements of the PDPA are complied with. Examples of policies and processes which should be re-examined are policies relating to the retention of records[14], disclosure of information to third parties[15] and security policies[16].

5. Prepare A Framework To Receive Data Access Requests ("DAR") And Data Correction Requests ("DCR")[17]

Organizations should be prepared to receive requests for access and/or correction as may be made by data subjects by (i) preparing DAR and DCR forms[18],and (ii) appointing a team of internal personnel to deal with any DARs and/or DCRs. The team of personnel should be adequately trained and equipped with sufficient knowledge and material i.e. guidelines and manuals, to respond to PDPA related requests and queries. Organizations may also wish to consider appointing a personal data protection officer.

D. FURTHER GUIDANCE

Organizations are advised to take steps to ensure that the above minimum recommended measures are put into place in preparation for the enforcement of the PDPA.

Organizations are also advised to be circumspect in terms of their implementation of the above measures, as it is likely that some of the measures taken may require readjustment based on the PDPA Regulations that are to be issued by the Commissioner.

FIMM may, where appropriate, issue updates to this Guidance Note from time to time.

Should you require further information or guidance in relation to the above, please contact Poh Khie Yee (Ext 300) Noraishah Hamid (Ext 303) or Sharon Kaur (Ext 309) of FIMM at 03-2093 2600.

---

[13] Pursuant to section 6 of the PDPA, organizations are required to obtain consent from prospective employees and existing employees prior to processing of personal data.
[14] e.g. in relation to the legally required retention periods and the destruction of both electronic and physical records thereafter.
[15] e.g. whether consent has been obtained and the conditions to be imposed prior to the disclosure of personal data.
[16] e.g. whether the security policy adequately covers the risk to electronic and physical personal data.
[17] Pursuant to S. 12 of the PDPA, data subjects are granted the right to access and correct their personal data.
[18] Such requests must be responded to within twenty one (21) days with an extension limited to fourteen (14) days.