e-CIRCULAR TO MEMBERS

CHARTERED TAX INSTITUTE OF MALAYSIA (225750-T)

e-CTIM PP 2/2014 **12 February 2014**

TO ALL MEMBERS

PUBLIC PRACTICE

Implementation of Personal Data Protection Act 2010 (PDPA)

The PDPA was gazetted on 10 June 2010 and was operative from 15 Nov 2013. It applies to any person who processes or who has control over or authorizes the processing of, any personal data in respect of commercial transactions, provided that

(a) *the person is established in Malaysia and the personal* data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or

(b) *the person is not established in Malaysia, but uses equipment* in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia.

The Act seeks to regulate the processing of "*personal data*" by "*data users*" in commercial transactions so as to protect the interest of "*data subjects*".

Personal data means any information in respect of commercial transactions which –

(a) is being **processed** wholly or partly by means of **equipment operating automatically** in response to instructions given for that purpose;

(b) is **recorded** with the intention that it should wholly or partly be processed by means of such equipment; or

(c) is recorded as **part of a relevant filing system** or with the intention that it should form part of a relevant filing system or with the intention that it should form part of a relevant filing system.

that **relates directly or indirectly to a data subject,** who is **identified or identifiable** from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010;

Data user means a person who either alone or jointly or in common with other persons **processes any personal data** or has **control** over or **authorizes the processing** of any personal data but does not include a data processor;

Data subject means **an individual** who is the **subject of the personal data**;

The contents of the PDPA are summarized below:

Part	Headings	Sections
I	Preliminary	1 – 4
II	Personal Data Protection Division 1-- Personal Data Protection Principles	5 - 12
	Division 2 -- Registration	13 - 20
	Division 3 -- Data User Forum And Code Of Practice	21 - 29
	Division 4 -- Rights Of Data Subject	30 - 44
III	Exemption	45 - 46
IV	Appointment, Functions And Powers Of Commissioner	47 - 60
V	Personal Data Protection Fund	61 - 69

VI	Personal Data Protection Advisory Committee	70 - 82
VII	Appeal Tribunal	83 - 100
VIII	Inspection, Complaint And Investigation	101 - 109
IX	Enforcement	110 - 127
X	Miscellaneous	128 - 144
XI	Savings And Transitional Provisions	145 - 146

The following are the relevant subsidiary legislations and notifications, all gazetted on 14 November 2013 and operative from 15 November 2013:

P.U. No.	Citation
(A) 335/2013	Personal Data Protection Regulations 2013 (the Regulation)
(A) 336/2013	Personal Data Protection (Class Of Data Users) Order 2013 (the Order)
(A) 337/2013	Personal Data Protection (Registration Of Data User) Regulations 2013
(A) 338/2013	Personal Data Protection (Fees) Regulations 2013
(B) 464/2013	Appointment of Date of Coming into Operation
(B) 465/2013	Appointment of Personal Data Protection Commissioner

Personal Data Protection Principles (PDPP)

S.5 of the PDPA provides that the processing of personal data by a data user shall be in compliance with the following PDPP:

(a) the General Principle;
(b) the Notice and Choice Principle;
(c) the Disclosure Principle;
(d) the Security Principle;
(e) the Retention Principle;
(f) the Data Integrity Principle;
(g) the Access Principle.

Details of the requirements under each respective Principle are found in S.6 to 8 respectively. More details of requirements under each Principle are found in the **Regulation**. For example:

- Under the *General Principle*, Reg. 3(1) provides that **a data user must obtain consent from a data subject** in relation to the processing of personal data in any form that such consent can be recorded and maintained properly by the data user
- Under the *Disclosure Princ*. Reg. 5 provides that the **data user must maintain a list of disclosure to third parties** for the purposes of paragraph 8(b) of the PDPA [the Disclosure Principle] in relation to personal data of the subject that has been or is being processed by him.

Inspection by Commissioner

Part III of the **Regulation** sets out the rules relating to inspection of the personal data system to be carried out by the *Personal Data Protection Commissioner* (which is provided for in S.101 of the PDPA). Regulation 14(2) provides for the following records (in relation to the respective principle) to be produced before the Commissioner when an inspection is carried out:

a) General Principle: The record of the consent from a data subject maintained in respect of the processing of personal data by the data user;
b) Notice And Choice Principle: the record of a written notice issued by the data user to the data subject in accordance;

c) Disclosure Principle: the list of disclosure to third parties for the purposes of para 8(b) of the PDPA in respect of personal data that has been or is being processed by him;

d) Security Principle: the security policy developed and implemented by the data user for the purpose of S9 of the PDPA;

e) Retention Principle: the record of compliance in accordance with the retention standard;

f) Data Integrity Principle: the record of compliance in accordance with the data integrity standard; or

g) Such other related information which the Commissioner or any inspection officer deems necessary.

Registration of data users

Division 2 of the PDPA (sections 13 to 20) applies to a data user who belongs to a class of data users who are specified in the **Personal Data Protection (Class Of Data Users) Order 2013**. Under the **Order,** the following broad headings for the classes of data users which must apply to be registered with the Commissioner are listed:

1. Communications
2. Banking and financial institutions
3. Insurance
4. Health
5. Tourism and hospitality
6. Transportation
7. Education
8. Direct selling
9. Services
10. Real estate
11. Utilities

Under item 9, Services, the following services were specified:

A **company** registered under the Companies Act 1965 (Act 125) or a person who entered into **partnership under the Partnership Act 1961** (Act 135) carrying on business as follows:

i) Legal;
ii) Audit;
iii) Accountancy;
iv) Engineering; or
v) Architecture.

The registration process and requirements are set out in the **Personal Data Protection (Registration Of Data User) Regulations 2013**; The Fees Structure are found in the Schedule to that Regulation.

Timeline for registration

Under S146(1), any person who processes any personal data or has control over or authorizes the processing of any such data at the date of coming into operation of the PDPA, is required to register as a data user in accordance with the provisions of the PDPA within 3 months of the date of coming into operation of the PDPA (i.e. by 15 Feb 2014).

Based on the wording of the Order, it would appear that data users who are providing (solely) tax consultancy services do not require to register with the Commissioner. The Institute was informed by certain Council member and Committee member that based on their verbal communication with the Department of Personal Data Protection (DPDP), there is no requirement for a taxation services provider to register. The Institute has written to

the DPDP for confirmation and members are advised that the aforesaid statements are subject to a written confirmation by the authority.

Nevertheless, members are reminded that S.13(2) of PDPA states that a data user who belongs to a class of user NOT specified in the Order must comply with ALL provisions of the PDPA other than the provisions of Division 2 (which deals with registration of data users) including the requirement under each PDPP as well as those relating to inspection by the Commissioner.

Members may refer to the official website of Department of Personal Data Protection for more information.