PERSONAL DATA PROTECTION ACT 2010: TAKING THE FIRST STEPS TOWARDS COMPLIANCE

(Akta Perlindungan Data Peribadi 2010: Mengambil Langkah Awal ke arah Pematuhan)

Farah Mohd Shahwahid & Surianom Miskam
Kolej Universiti Islam Antarabangsa Selangor

ABSTRACT

With the coming into force of the Personal Data Protection Act 2010 (PDPA 2010) on 15 November 2013, business entities (data users) are now obligated to comply with the principles of data protection enshrined in the Act. The aim of PDPA 2010 is to ensure that personal data of consumers (data subjects) that are collected, stored and used by the data user is being handled in the correct manner. The Act contains seven principles of data collection in line with data protection legislations worldwide. This study aims to discover whether the provisions of PDPA have been complied with by the data users. This will be done by looking at the provisions from the Act regarding the principles of data protection as well as the duties for compliance to the legislation. Furthermore, the privacy policy from selected data user business entities from selected industries are examined. The study also seeks to discover what are the barriers that need to be overcome in implementing PDPA 2010 successfully.

***Keywords*:** Personal Data Protection Act 2010; personal data; data user; data subject; compliance

ABSTRAK

Dengan berkuat kuasanya Akta Perlindungan Data Peribadi 2010 pada 15 November 2013, semua entity perniagaan (pengguna data) diwajibkan mematuhi prinsip-prinsip berkaitan perlindungan data yang terkandung dalam Akta tersebut. Objektif utama Akta ini adalah untuk memastikan bahawa segala data peribadi orang awam (subjek data) yang dikumpul, disimpan dan digunakan oleh pengguna data dalam aktiviti komersial dikendalikan mengikut prosedur yang ditetapkan. 7 prinsip perlindungan data peribadi yang digubal selari dengan perundangan perlindungan data yang digunapakai di seluruh dunia. Kajian ini akan melihat kepada pematuhan pengguna data kepada peruntukan-peruntukan yang terkandung dalam Akta ini dengan melihat kepada peruntukan-peruntukan berkaitan dalam Akta berkenaan prinsip-prinsip perlindungan data dan tanggungjawab pengguna data terhadap pematuhan Akta ini. Di samping itu, polisi privasi data peribadi beberapa entiti perniagaan yang tertakluk kepada Akta ini akan dikaji untuk melihat sejauhmana mereka mematuhi kehendak Akta ini. Kajian juga cuba mengenalpasti apakah halangan yang perlu di atasi untuk memastikan Akta ini dapat dikuatkuasakan dengan berkesan.

***Kata kunci**: Akta Perlindungan Data Peribadi 2010; data peribadi; pengguna data; subjek data; pematuhan undang-undang*

1. INTRODUCTION

Information is a valuable commodity these days. Information is also seen as a controversial tool of modern life. With vast quantities of information belonging or regarding to individuals being held by various business entities, many issues arise as to the mechanism in handling all this personal information. Matters pertaining to who holds this information, how they hold it, and in what circumstances they use it and/or pass it on to others, has been the subject of detailed legislation and regulation for many years.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), adopted by the Council of Europe in 1981 was the first legal instrument to guarantee the protection of personal data, as a separate right granted to an individual. This convention obliges the signatories to enact legislation concerning the automatic processing of personal data. At the same time, the Organization for Economic Co-operation and Development (OECD) issued guidelines to its members, which urged them to introduce measures to protect personal information. The European Commission realised that diverging data protection legislation amongst EU member states impeded the free flow of data within the EU. In 1995, the EU Data Protection Directive was enacted setting out the data protection principles that EU member states must incorporate into their national data protection laws.

In 1973, Sweden became the first country to adopt personal data protection legislation with the passing of the Data Act. That legislation became the first national law that implemented what we now recognize as the basic principles of data protection. Four decades later, almost 100 other countries have followed suit.

2. PERSONAL DATA PROTECTION IN MALAYSIA

As far as Malaysia is concerned, with the passing of Personal Data Protection Act 2010 (PDPA) on June 2010 Malaysia becomes the first ASEAN nation to introduce such laws into the region, and after a long wait, this law has now became enforceable on the 15th November 2013. The coming into effect of the law is almost one year after the Act was scheduled to take effect on January 1, 2013, but delayed due to legal formalities. The bill was first drafted in 2001 and was originally expected to be implemented early 2010. It was initially scheduled to be passed August 16 2013, with businesses using personal data required to register themselves with the Personal Data Protection Department of Malaysia by November 15, 2013. (The Malay Mail Online, 15 November 2013)

The PDPA was formed primarily to regulate the processing of personal data collected for commercial purposes and all other matters connected or incidental to consumers' personal data. The PDPA also aims to safeguard consumers' rights regarding their personal data. The Act requires companies and organisations that handle consumers' personal data in commercial transactions (data users) to notify them and obtain their consent for any collecting and processing of their personal information.

The PDPA is applicable to a data user which is defined in section 4 of the Act as 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. In short, a data user is a person who processes or controls or authorizes the processing of personal data. Abu Bakar Munir (2012) adds that a data user must be a legal

person. The term legal person would cover individuals, companies and other corporate and unincorporated entities.

The PDPA is only applicable for data or information that falls under 'personal data'. Section 4 of the act defines personal data as any information in respect of a commercial transaction, 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 from part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information.

The Act also provides the definition for data subject under section 4 as an individual who is the subject of the personal data. This means that data subject is the owner of the personal data that is being processed by the data user. Referring to the definitions, for a particular data or information to qualify as personal data under the PDPA, it must be shown that the data subject can be identified or is identifiable from the data in question. In simpler words, the data that was processed by the data user can be traced back to a particular individual, i.e. the data subject. Among data or information that would qualify as personal data would include the name, identification numbers, addresses, telephone numbers, bank account numbers and even place of work or place of birth. Sometimes, one data alone does not make an individual identifiable, but a series or a combination of data does so.

Abu Bakar Munir (2012) further explains this by saying that an identifiable person appears to be the one whose separate identity is ascertainable but who is not known in person. He or she may be traceable by virtue of certain factors. It is suggested that a person is identifiable where there is sufficient information either to contact him or to recognize him by picking him out in some way from others. Furthermore, a person is identifiable if his identity can be ascertained from the information held plus the results of reasonable enquiries which are made either by the data user or another.

The PDPA is applicable to any person who processes data either by automatic means or manually. Processing is defined in section 4 to include the 'collecting, recording, holding, or storing the personal data or carrying out any operation or set of operations on the personal data, including the organization, adaptation or alteration or personal data, the retrieval, consultation or use of personal data, the disclosure of personal data by transmission, transfer, dissemination or otherwise making available, or the alignment, combination, correction, erasure or destruction of personal data. The definition was deliberately framed broadly to include all possible activities of a data user. Automatic means of processing data would include the recording and storing of personal data in a computer or online database, as well as the use or disclosure of personal data on the data user's email, mailing list or website. Examples of manual processing of personal data would include the collecting of consumers' business cards or application forms, keeping consumers personal information in logbooks or filing cabinets and erasing or shredding documents containing the personal information of consumers.

2.1 The provisions of the PDPA 2010

Compliance to the PDPA is by following the seven data protection principles which are expressly and clearly stated in the provisions of the Act. Section 5(1) lists down the data

protection principles while section 5(2) of the Act mentions that contravention of the data protection principles shall be punishable by fine, imprisonment or even both.

The first principle of data protection is the General Principle section 6 which provides that no personal data about a data subject is to be processed unless the data subject has consented to the processing. It also states that a data user shall not process any sensitive personal data of a data subject unless it is in accordance with section 40 of the same Act. Section 6(3) further states that any personal data shall not be processed unless the personal data is processed for a lawful purpose directly related to the activity of the data user, the processing of the personal data is necessary for, or directly related to that purpose, and the personal data is adequate but not excessive in relation to that purpose.

Section 7(1) discusses the second data protection principle which is the notice and choice principle. The provision requires the data user to inform the data subject by giving a notice in writing that

(a) That personal data of the subject is being processed by or on behalf of the data user, and shall provide a description of the personal data to that data subject;
(b) The purposes for which the personal data is being or is to be collected and further processed;
(c) Of any information available to the data user as to the source of that personal data;
(d) Of the data subject's right to access to and to request correction of the personal data user with any inquiries or complaints in respect of the personal data;
(e) Of the class of third parties to whom the data user discloses or may disclose the personal data;
(f) Of the choices and means the data user offers the data subject for limiting the processing of personal data, including personal data relating to other persons who may be identified from that personal data;
(g) Whether it is obligatory or voluntary for the data subject to supply the personal data; and
(h) Where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he fails to supply the personal data.

This principle requires a company to have a privacy policy statement, which contains all the matters stated above. All of the requirements must be complied with, not a selected few. This provision also requires that the written notice shall be in both Bahasa Melayu and English. If the data users wish, they can also provide the privacy policy in other languages as well. The data user must also ensure that consumers are provided with the means to choose the privacy policy.

Section 8 of the PDPA prohibits the disclosure of personal data for other purposes without the consent of the data subject. The prohibition covers two aspects, which are firstly, the purpose for the disclosure and secondly to whom is the disclosure of personal data made to. For the first part of the prohibition, data users are only allowed to disclose the personal data for the purpose or directly related purpose that the data was collected for in the first place. However, the PDPA does provide certain exceptions where personal data may be disclosed without the consent of the data subject. These exceptions are laid down in section 39 which includes that the disclosure is necessary for the purpose of preventing or detecting a crime, or for investigation purposes or where disclosure of personal data is required or authorized by or under any law or court order (section 39 (b); the data user has acted in the reasonable belief that he had a right to disclose the personal data to the other person or had

acted in the reasonable belief that he would have had the consent of the data subject if the data subject had known of the disclosure and the circumstances of such disclosure (section 39 (c) and (d)); and lastly the disclosure was justified as being in the public interest.

For the second part, data users are only allowed to disclose the personal data to any third party or class of third parties that are stated in the written notice provided to the data subject. This is to ensure that the data subject has been made aware of the existence of the third party/parties and the consent of the data subject was obtained before the personal data can be processed by such third party/parties.

Section 9 of PDPA governs the security principle which requires a data user to take practical steps to protect the personal data being processed from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. To comply with this principle, protection must be given in regard to the nature of the personal data, the place or location the data is stored, the security measures which are incorporated to the equipment where the data is stored, the measures taken to ensure the integrity of the personnel having access to the data as well as the measures taken to ensure secure transfer of the data. In cases where data processing is done on behalf of the data user by a data processor, Section 9(2) requires the data user to take steps to ensure that the data processor provides sufficient guarantees in respect of security measures governing the processing of personal data, and takes reasonable steps to ensure compliance to aforementioned measures. In complying with the security principles, the measures taken by the data user would differ and depend on the industry the data user conducts its commercial activities as well as the type of personal data that is being processed. For certain industries which deal with sensitive, confidential and valuable personal data on a daily basis, such as the banking, insurance, health and communication industries, data users are expected to take high level security measures to safeguard the personal data in order for them to fulfill the requirements of section 9. Examples would include personal details concerning banking transactions, insurance policies, health records and medical history of patients and the telephone numbers and addresses of clients of the data users.

This principle clearly states 'practical steps'. The data user must only take measures that commensurate with the risks represented by the processing of, or the nature of the data together with the cost of implementing such security measures. Data users must strike a balance between the seriousness of the consequences of failure in security and the price of putting into place the security measures.

The retention principle endowed in section 10 of the PDPA requires that personal data is not retained or kept by the data user for a period longer than necessary for the fulfillment of the purpose it was processed. It is the responsibility of the data user to destroy or permanently delete the personal data. The words 'shall not be kept' in that section seem to indicate that it is mandatory for the data user to dispose the data when it is no longer needed for its purpose. The Act is silent on the period for deletion or how for the data user to determine when to dispose of the data.

Section 11 explains the data integrity principle, a crucial element in personal data protection law. This provision requires the data user to take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up to date having regard to the purpose, including any directly related purpose for which the personal data was collected and later processed. This requirement shows the importance of the data user ensuring that no personal data are inaccurate, incomplete or obsolete.

Any data subject must be given the right of access to the personal data held and processed by the data user. If the personal data is inaccurate, the data subject must be able to correct the data to give effect section 12.

2.2 Rights of Individuals (Data Subjects)

In relation to the processing of personal data of individuals, certain statutory rights are provided under the PDPA. The six rights are the right to be informed, right of access to personal data, right to correct personal data, right to withdraw consent, right to prevent processing which is likely to cause damage or distress and right to prevent processing for the purpose of direct marketing.

The right of access to personal data gives effect to the access principle. The provisions governing this right are Section 30-33. Section 30 (1) provides that an individual is entitled to be informed if his personal data is being processed by or on behalf of the data user. Section 30(2) says that upon payment of a prescribed fee, a requestor may make a data access request in writing to the data user for information of the data subject's personal data that is being processed by the data user and for that information to be communicated to him in an intelligible form. However, section 32 the n lays down the circumstances where a data user may refuse to comply with that request.

The right to correct personal data is also provided in the Act under sections 34-47. Section 34 (1) says that where a requestor of a data access request or the data subject himself considers that personal data being held by the data user is inaccurate, the requester or the data subject, may make a data correction request in writing to the data user for necessary amendments to be made to the personal data. However, section 36 states that in certain circumstances, the data user may refuse to comply with a data correction request. To prevent such refusal, it is advised that the person seeking the data correction to supply the necessary evidence to prove the inaccuracy of the personal data.

The right to withdraw consent for processing data is guaranteed under section 38 which expressly states that the data user shall cease the processing of personal data, upon receiving a notice in writing for him to do so.

Section 42 then further goes on to explain another right of a data subject which is the right to prevent processing of any personal data that is likely to cause damage or distress to the data subject or to any other person. This provision also gives a right to the data subject to prevent the data user from collecting, holding, processing or using his personal data. For this provision to be applicable, the data subject must prove that the collecting, holding, processing or use of that personal data causes or is likely to cause damage or distress, and the damage or distress caused must be substantial and unwarranted. As the words 'substantial' and 'unwarranted' is not defined in the Act, it can be interpreted to suit the particular type of personal data or industry in that particular situation.

Another right accorded by the PDPA is the right to decide whether or not they wish to have their personal information used for direct marketing purposes. Section 43(1) states that a data subject, may, by submitting a notice in writing to the data user, require the data user to cease or not proceed with the processing of his personal data for direct marketing purposes. Direct marketing is defined in the PDPA to mean the communication by whatever means of any advertising or marketing material which is directed to particular individuals. This right can be exercised by the data subject at any time, even if they have initially consented to the use of their personal data, this consent can be later on revoked. Businesses that operate a

direct marketing approach should pay extra attention to this clause as it cannot be assumed that once consent has been given by a data subject, that the consent will be continuous. Once consent has been revoked, no direct marketing material of any form should be sent to the data subject anymore. This would include but not limited to letters, brochures and catalogues both in paper and paperless form. This provision is unique in the sense that it is applicable to not only prevent the sending and receiving of marketing communication but also can be used to stop the profiling, screening or data mining activities involving the data subject's personal data.

2.3 Penalty for Non-Compliance

Failure to comply with the provisions of this legislation is a punishable criminal offence. Section 135 states that prosecution under the PDPA must be instituted by, or with the written consent of the public prosecutor. Section 135 gives the authority to Sessions Court to try any offence under the PDPA and to impose punishment for any such offences under the PDPA. Non-compliance of the PDPA is punishable by a fine or to imprisonment or to both. This punishment is clearly stated under section 5(2) of the PDPA which states that subject to the exemptions under section 45 and 46, a data user who contravenes the personal data protection principles commits an offence and shall, upon conviction, be liable to a fine not exceeding RM300,000 or to imprisonment not exceeding two years, or both.

Other offences under the PDPA by those who qualify to be data users include the processing of personal data without having a certificate of registration (section 16) and the continuing to process personal data after the revocation of registration as data user (section 18). Another offence under the legislation is stated under section 130 which provides that a person commits an offence when he, either knowingly or recklessly, without the consent of the data user, collects, discloses, or procures the disclosure of data to another person. These offences upon conviction carries the punishment of fine not exceeding RM500,000 or to an imprisonment for a term not exceeding three years, or both.

Section 38 provides that data users who fail to cease the processing of personal data upon receiving notice from the data subject withdrawing consent to the processing of his personal data, commits an offence, and upon conviction is liable to a fine not exceeding RM100,000 or imprisonment up to one year, or both.

Another offence under PDPA is stated under section 40, the processing of sensitive information contravening the conditions stated in the Act. This offence, upon conviction is liable to punishment of fine not exceeding RM200, 000 or to imprisonment for a term not exceeding two years, or both.

Offences of data user's refusal to comply with a data correction request by the data subject, non-compliance with any code of practice applicable to a data user (Section 29), and a data user's continuous processing of personal data after withdrawal of consent from data subject (Section 38) are all punishable by a fine not exceeding RM100, 000 or imprisonment not more than 1 year, or both.

2.4 Privacy Policy: Compliance by Business Entities

The enforcement of PDPA on the 15 November 2013 also introduced some subsidiary legislations including the Personal Data Protection (Class of Data Users) Order 2013 (PDPO 2013). This new regulations require certain class of data users to register with the Personal

Data Protection Commissioner. These selected data users are from the following 11 industries:

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

The law requires that business entities and service providers under these categories to comply within three months from the date of the coming into effect of the legislation. By looking at the list, this would include data users like banks, financial institutions, telecommunication firms, insurance companies, private hospitals, private schools, colleges and universities, commercial airlines, law firms, real estate agencies, and utilities' providers such as Tenaga National Berhad, ASTRO and SYABAS. Besides registration, enforcement of PDPA would require compliance to the personal data principles. The initial step to be taken by data users is by having a privacy policy in place, where the data user guarantees to take steps to comply with the seven data protection principles.

Referring to the websites of some selected data users, the privacy policy of these selected data users were analysed to see if they complied with the requirements of PDPA. The findings are summarized as follows:

2.4.1 Maybank (Malayan Banking Berhad)

The privacy notice of Malayan Banking Berhad is accessible through its website www.Maybank2u.com. It is available in both English and Bahasa Melayu. The notice explains that it collects, uses, maintains and discloses customers' personal data in respect of commercial transactions and that it takes steps to safeguards the personal data collected from their customers. The notice also lists down, non-exhaustively, the types of personal data collected from the customers. The privacy notice contains provisions regarding all seven principles of data protection. There are provisions explaining the use the personal data processed and while it undertakes to keep data confidential, the notice admits that there are circumstances where the data will be disclosed to third parties. A provision is also included allowing data subjects (customers of Maybank) to amend any incorrect data being processed, as well as the actions to be taken by the data subject to amend or correct the data.

2.4.2 CELCOM

The privacy policy of CELCOM is available online through its website and expressly states that the Customer Service Division is responsible for the customer access and correction of personal data, notice and choice process to limit processing of personal data and the Privacy Department in Legal Division is responsible for the monitoring the administration

of this notice and monitoring its compliance. The privacy policy includes provisions on all the data protection principles, where CELCOM promises compliance. The policy also has a clause regarding the processing of sensitive personal data where it states "that it does not process any sensitive personal data in its ordinary course of business but if the need arises, CELCOM will obtain explicit consent from the customer before or when it processes sensitive personal data. At this point, CELCOM may process personal data without the customer's consent only in limited circumstances as permitted by law".

2.4.3 Telekom Malaysia Berhad

Similar to other data users, Telekom has prepared a privacy policy in line with the requirement of PDPA. The policy contains provisions detailing the company's processing of customers' personal data and all seven principles of personal data are dealt with in the policy. While promising to safeguard the personal data, the company admits to using the data collected for purposes mentioned in the policy. The policy contains information on how data subjects (referred to as 'Members" in the policy) may choose to 'opt out" from receiving mail, and how the ycan modify their information or make any other necessary changes.

3. LIMITATIONS AND CHALLENGES AHEAD

Section 2(2) of PDPA provides that the Act applies to a data user in multiple ways. Firstly, where the data user is established in Malaysia and the data user processes data. Secondly, when the data user that is established in Malaysia, employs or engages someone to process personal data. Thirdly, when a data user who is not established in Malaysia, uses equipment in Malaysia to process personal data. Therefore, it can be said that the applicability of this Act is limited to Malaysian data users or at least to data that was processed in this country.

A severe limitation of this Act that has also been a subject of criticism by many is the fact that this Act, as stated in section 3(1) does not cover both the Federal and State governments of Malaysia. As a huge amount or personal data is processed by government agencies, the exclusion of these entities would surely have implications on the successful implementation of this law.

Section 3(2) also excludes data wholly processed outside of Malaysia unless that personal data is intended to be further processed in Malaysia. The effect of this is that the PDPA is not applicable to internet based data gatherers, unless the data collected is used or is to be used in Malaysia. For example, if a Hong Kong based bank (the data user) gathers information from Malaysian consumers (the data subjects) through the internet, the PDPA is not applicable unless the data collected is used or is intended to be used in Malaysia.

Another important element in discussing the applicability of PDPA is that this law is only applicable to the processing of personal data in respect of commercial transactions. Therefore, any personal processed for non-commercial or private use is exempted from this legislation. Section 4 of the PDPA defines commercial transaction to mean any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agencies, investments, financing, banking and insurance. The definition provided by the Act does not include credit reporting which is under the purview the Credit Rating Agency Act 2010.

With the fast changing world of information and communication technology where international data transfer is unavoidable it has increased the complexity of personal data management itself from the moment data is collected, used, stored, and destroyed. The PDPA is equally applicable to all customers, employees, and third party service providers that handle personal data. Overall, companies businesses will also be affected as processes will be required to be refined to comply with the requirements of the Act.

Besides the issue of applicability of PDPA, another challenge that is being faced is the lack of knowledge on PDPA specifically or on the concept of personal data protection as a whole. Many business owners are clueless as to their status as data users. They are unsure if they fall under the purview of the PDPA and if they are, what are the steps that need to be taken by them. Business owners are still unsure of what constitutes personal data? For example, a wedding planner deals with many parties, from the couple getting married to the various contractors that he engages for wedding related services. Is the wedding planner breaking the law by keeping a collection of pictures and videos of his clients' weddings? It is unsure if the Act applies in this context. (The Star Online, 2 February 2014)

Another aspect that impedes the successful implementation of PDPA is the limitation in terms of data users being 'technology savvy'. According to the managing director of a security solution company, Goh Chee Hoh "it is not easy now for businesses to equip themselves with the proper tools to help them to secure their customers' personal data because people today are using a diverse set of mobile devices, operating systems and consumer apps to handle sensitive data". (The Star Online, 2 February 2014)

While much effort to increase knowledge awareness on PDPA has been conducted in the forms of seminars and public awareness campaigns through the media, it is clear that much more needs to be done. For many of the multinational companies, compliance with the PDPA should not be a big problem as they already have in place a global policy that just needs to fit to the Malaysian requirements. Those who seem to struggle the most with compliance are the small and medium enterprises (SME). (The Star Online, 2 February 2014)

This view is supported by Kuok Yew Chen, a lawyer at Christopher & Lee Ong, one of many law firms providing legal consultancy over the PDPA. Kuok believes that many companies already have some sort of privacy policy in place. "Generally, the multinationals would already have global privacy policies and so they would simply need to adapt these to meet the requirements of Malaysia's PDPA. It is, perhaps, the small- and medium-enterprises that would be least prepared, given that not many would have internal policies or procedures on privacy and protection of personal data," said Kuok. (The Star Online, 2 February 2014)

4. CONCLUSION AND RECOMMENDATIONS

The PDPA has already been enforced and business entities and service providers are required to register by 15 February 2014 or face penalties under section 16(4) of the PDPA. Since the grace period of three months has expired, it means that this is the time for enforcement. Relevant parties and the authority should take measures to identify the gaps to meet the legal requirements and industry standards in order to develop a strategic roadmap to address the gaps and to develop structure, roles and responsibilities, policies and procedures to be applied by all affected parties. More important, audit processes and systems to assess compliance with policies, standards, and legal requirements should be set up and enforced to maintain strict compliance of the law.

5. REFERENCES

Businesses in the dark over PDPA, retrieved from: http://www.thestar.com.my/News/Nation/2014/02/02/Businesses-in-the-dark-over-the-PDPA/, accessed on 20 April 2014.

Comply with Act or face action, data users warned, retrieved from: http://www.thestar.com.my/News/Nation/2014/02/02/Comply-with-Act-or-face-action-data-users-warned/, accessed on 24 April 2014.

Data Protection Act gazzetted effective today, retrieved from: http://www.themalaymailonline.com/malaysia/article/data-protection-act-gazetted-effective-today, 15 November 2013 accessed on 11 May 2014.

Data users must register with Personal Data Protection Dept by Feb 15, retrieved from: http://www.thestar.com.my/News/Nation/2014/02/06/Data-protection-Feb15/, accessed on 2 May 2014.

http://celcom.com.my, retrieved on 2 May 2014.

http://pdp.gov.my, retrieved on 2 May 2014.

http://www.maybank2u.com.my, retrieved on 2 May 2014.

http://www.tm.com.my, retrieved on 4 May 2014.

Greenleaf, Graham, Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories, September 10, 2013, Journal of Law, Information & Science, 2013 UNSW Law Research Paper No. 2013-40.

Munir, A. B. (2010). The Personal Data Protection Bill 2009, Malayan Law Journal Articles [2010] 1 MLJ cxix.

Munir, AB. (2012). *Personal Data Protection Act: Doing Well by Doing Good,* Malayan Law Journal Articles *[2012] 1 MLJ lxxxiii.*

Protecting Your Personal Data, retrieved from http://www.thestar.com.my/News/Nation/2012/02/12/Protecting-your-personal-data/, accessed on 24 April 2014.

NUBE: Bank staff forced to give up their personal info, retrieved from: http://www.thestar.com.my/News/Nation/2014/02/02/Nube-Bank-staff-forced-to-give-up-their-personal-info/ accessed on 2 May 2014.

Website of Foong Cheng Loong (advocate & Solicitor) Legal Articles on Intellectual Property, Social Media, Data Privacy, Franchise and Others retrieved from: http://foongchengleong.com/2013/11/enforcement-of-the-personal-data-protection-act-2010-4/ accessed on 24 April 2014.

Yong, P. K. (2009). Privacy and Personal Data Protection In The Malaysian Communications Sector -- Existing In A Void? Malayan Law Journal Articles [2009] 5 MLJ ciii.

You can't call me anymore, retrieved from: http://www.thestar.com.my/News/Nation/2014/03/09/You-cant-call-me-any-more/, accessed on 2 May 2014.

Your data is your own, retrieved from: http://www.thestar.com.my/News/Nation/2014/02/02/Your-data-is-your-own-Check-before-giving-your-consent-says-PDP-commissioner/, accessed on 24 April 2014.

Farah Mohd Shahwahid
Surianom Miskam
Department of Business Management
Faculty of Management and Muamalah
International Islamic University College Selangor
farahms@kuis.edu.my
surianom@kuis.edu.my