NEW ZEALAND CENTRE FOR PUBLIC LAW
Te Wānanga o ngā Kaupapa Ture ā Iwi o Aotearoa

New Zealand Journal of Public and International Law

VOLUME 9 • NUMBER 1 • JUNE 2011

THIS ISSUE INCLUDES CONTRIBUTIONS BY:

The Hon Sir Anthony Mason AC KBE
Stephen Rivers-McCombs
Zuryati Mohamed Yusoff
Joel Colón-Ríos
Cristiano d'Orsi

Victoria
UNIVERSITY OF WELLINGTON
Te Whare Wānanga
o te Ūpoko o te Ika a Māui

FACULTY OF LAW
Te Kauhanganui Tātai Ture

Faculty of Law
Victoria University of Wellington
PO Box 600
Wellington
New Zealand

June 2011

The mode of citation of this journal is: (2011) 9 NZJPIL (page)

The previous issue of this journal is volume 8 number 2, December 2010

ISSN 1176-3930

Printed by Geon, Brebner Print, Palmerston North

Cover photo: Robert Cross, VUW ITS Image Services

CONTENTS

The **New Zealand Journal of Public and International Law** is a fully refereed journal published by the New Zealand Centre for Public Law at the Faculty of Law, Victoria University of Wellington. The Journal was established in 2003 as a forum for public and international legal scholarship. It is available in hard copy by subscription and is also available on the HeinOnline, Westlaw and Informit electronic databases.

NZJPIL welcomes the submission of articles, short essays and comments on current issues, and book reviews. Manuscripts and books for review should be sent to the address below. Manuscripts must be typed and accompanied by an electronic version in Microsoft Word or rich text format, and should include an abstract and a short statement of the author's current affiliations and any other relevant personal details. Authors should see earlier issues of NZJPIL for indications as to style; for specific guidance, see the New Zealand Law Style Guide 2010. Submissions whose content has been or will be published elsewhere will not be considered for publication. The Journal cannot return manuscripts.

Regular submissions are subject to a double-blind peer review process. In addition, the Journal occasionally publishes addresses and essays by significant public office holders. These are subject to a less formal review process.

Contributions to NZJPIL express the views of their authors and not the views of the Editorial Committee or the New Zealand Centre for Public Law. All enquiries concerning reproduction of the Journal or its contents should be sent to the Student Editor.

Annual subscription rates are NZ$100 (New Zealand) and NZ$130 (overseas). Back issues are available on request. To order in North America contact:

Gaunt Inc
Gaunt Building
3011 Gulf Drive
Holmes Beach
Florida 34217-2199
United States of America
e-mail info@gaunt.com
ph +1 941 778 5211
fax +1 941 778 5252

Address for all other communications:

The Student Editor
New Zealand Journal of Public and International Law
Faculty of Law
Victoria University of Wellington
PO Box 600
Wellington
New Zealand
e-mail nzjpil-editor@vuw.ac.nz
fax +64 4 463 6365

THE MALAYSIAN PERSONAL DATA PROTECTION ACT 2010: A LEGISLATION NOTE

Zuryati Mohamed Yusoff*

Modern information technology allows people to do things that would not have been possible before in a fast and easy way. The significant role of information in the global economy and the implications of collection, use, processing and disclosure of personal data have raised concerns over the issues which need addressing in terms of protection. Data protection law was developed to protect personal information from being misused and manipulated. The Malaysian Personal Data Protection Act 2010 was modelled on international data protection laws with focus on the protection of personal data in commercial transactions. This note will scrutinise the Personal Data Protection Act 2010 from a privacy point of view and suggest ways to overcome the shortcomings. It is suggested that the limit of commercial transactions should be removed to include non-commercial transactions if the Act is to protect personal data in its widest sense.

I Introduction

In the digital age, data or information has become an especially valuable, yet vulnerable commodity.[1] The significant role of information in the global economy and the implications of the collection, use, processing and disclosure of personal data have raised concerns over the ways in which the personal data can be protected. For Malaysia, data protection, or information privacy, is relatively new. As it develops, it demands specific law to provide a secure environment for personal data in electronic transactions.

In Malaysia, the Constitution has not made privacy a fundamental human right equivalent to other rights guaranteed under it. However, it does provide for several privacy-related rights,

* PhD Researcher at Victoria University of Wellington, New Zealand. I would like to thank Professor Tony Angelo, Dr Nicole Moreham and the anonymous reviewer for their useful comments on an earlier draft of this note.

1 In the Explanatory Statement of the Personal Data Protection Act 2010 (PDP 2010) data is clearly regarded as a valuable commodity.

including liberty of the person,[2] freedom of movement[3] and freedom of assembly, speech and association.[4] Additionally, English common law principles are widely applicable to privacy-related cases such as defamation, nuisance, trespass and breach of confidence.

More than a decade ago, the Multimedia Super Corridor Malaysia or "MSC" project[5] was formulated with the full support of the Malaysian Government to transform the nation into a knowledge-based economy. As part of the programme, a data protection law was introduced to create a legal and regulatory framework for the project. The proposed Act was tabled a number of times in Parliament.[6] It was finally passed on 5 April 2010,[7] and became law on 10 June 2010.[8]

The purpose of this note is to discuss this new Personal Data Protection Act 2010 (PDP 2010)[9] from a privacy protection perspective and to examine its scope and its limitations in regulating the handling and controlling of personal data. The protections available in processing, holding, collecting and using any data pertaining to an individual person will be scrutinised. The paper also makes comparison with the United Kingdom and Hong Kong Data Protection legislation and highlights the international features reflected in the PDP 2010 particularly the OECD Guidelines, the Council of Europe Convention, the EU Data Protection Directives and the APEC Privacy Framework. The discussion concludes with suggestions for overcoming the Act's perceived flaws. This analysis shows that the PDP 2010 is a law that outlines data protection principles in a generic form but does not provide protection in terms of damages and injunction to individuals whose data has been encroached upon and is not dedicated to the protection of individual privacy.

II Overview of the Act

Initially the PDP 2010 was drafted to replicate laws on personal data from other jurisdictions in respect of the personal data protection principles with modifications to suit local needs and

---

2 The Federal Constitution of Malaysia, art 5, provides that: "No person shall be deprived of his life or personal liberty save in accordance with law."

3 The Federal Constitution of Malaysia, art 9, provides that: "No citizen shall be banished or excluded from the Federation" and that "Every citizen has the right to move freely throughout the Federation and to reside in any part thereof."

4 The Federal Constitution of Malaysia, art 10 states that: "Every citizen has the right to freedom of speech and expression; to assemble peaceably and without arms; and to form associations."

5 The project was introduced by the Malaysian Government in 1996.

6 The first Bill was introduced in 1998 and a redrafting of the Bill took place in 2001. Both of the Bills were tabled and debated in the Parliament.

7 See "Parliament: Personal Data Protection Bill Passed" (2010) The Star Online <http://thestar.com.my>.

8 As at 1 April 2011 the PDP 2010 is not in force.

9 The PDP 2010 was given the Royal Assent on 2 June 2010 and was gazetted on 10 June 2010.

circumstances. The Act's dominant influences are from the Hong Kong Personal Data (Privacy) Ordinance 1995 and the Data Protection Act 1998 (UK). The personal data protection principles are structured in terms which are identical to those of both pieces of legislation and the PDP 2010 contains all those principles in order to satisfy minimum requirements for the law governing collection and processing of personal data.[10]

The preamble of the PDP 2010 states that it is an Act "to regulate and protect the process of personal data from being misused through commercial transactions and matters relating thereto". Thus, it aims only to safeguard confidentiality in the handling of an individual's personal data and preventing misuse of that data in relation to commercial transactions.

A Key Definitions

1 Personal data

The term "Personal data" is defined to mean:[11]

> 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,
>
> 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 the data user, including any sensitive personal data and expression or 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 2009.

10 European Union Data Protection Directive 1995, art 25.

11 Personal Data Protection Act 2010, s 4.

Therefore, personal data includes any information or opinion as far as it relates to an identified or identifiable living person[12] and processed both manually and electronically.[13]

2 *Processing*

The Act defines "processing" to mean:[14]

> collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data including-
>
> (a) the organization, adaptation or alteration of personal data;
>
> (b) the retrieval, consultation or use of personal data;
>
> (c) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or
>
> (d) the alignment, combination, correction, erasure or destruction of personal data.

3 *Commercial transactions*

The PDP 2010 provides a regulatory framework for the processing of personal data in commercial transactions.[15] Thus, the meaning of "commercial transactions" is crucial in order to understand the nature of the personal data protected under the Act. Commercial transactions refers to:[16]

> … any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments financing, banking and

---

12 It refers to a data subject which is defined by s 4 to be an individual who is the subject of the personal data. The word "individual" here clearly points to living person. The term "data user" refers to a person who either alone, jointly, or in common with other persons processes any personal data or has control over or authorises the processing of any personal data, but does not include a data processor.

13 Section 4 defines "relevant filing system" as any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set of information is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

14 Personal Data Protection Act 2010, s 4.

15 The word "commercial" has not been defined clearly in Malaysian legislation of a commercial nature. See, the Contracts Act 1950, the Sale of Goods Act 1957, the Banking and Financial Institutions Act 1989, the Consumer Protection Act 1999 and the Hire Purchase Act 1967.

16 Personal Data Protection Act 2010, s 4. The definition of personal data also excludes the information processed for the purpose of credit reporting business and as such is redundant with the definition of "commercial transaction".

insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agency Act 2009.

By the definition, the data and confidential information of online consumers fall under the meaning of "commercial transactions" intended by the Act. Thus, if a customer provides their name, address, contact number and some other information to complete a transaction, that data or personal information is protected under the Act. The company receiving the information is under an obligation to keep the data and is allowed to use or disseminate the data only with the consent of the data subject. Conversely, the data of a patient in relation to medical treatment will not fall under this definition as it does not have commercial features. Nevertheless, that data merits similar protection for the reason that it is easily abused and misused through online transactions. Similarly, the PDP 2010 has no application to personal data collected through social media networking websites such as *Facebook*, *Twitter* and *MySpace* because that data is not as a result of commercial transactions.[17] The fact that those data are being stored and kept by foreign online providers which do not have local centres of data processing justifies its exclusion from the scope of the Act.[18]

4 Credit Reporting Agency

In relation to the definition of "commercial transactions", it is interesting to point out the definition of "credit reporting agency" as the PDP 2010 expressly excludes its application to such business. Under the Credit Reporting Agencies Act 2010 (CRA 2010)[19] the consent of an individual is needed before the financial information can be displayed by credit-reporting agencies.[20] In its explanatory statement, it is stated that the purpose of the legislation is "to provide for the registration and regulation of persons carrying on credit reporting businesses and for matters connected therewith and incidental thereto".

---

17 See also Foong Cheng Leong "Personal data and the law" (2010) The Star Online <www.thestaronline.com>.

18 It is expressly provided under s 3(2) of the PDP 2010 that "This Act shall not apply to any personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia."

19 The Credit Reporting Agencies Act 2010 adopted the New Zealand Credit Reporting Privacy Code 2004 which is established under the Privacy Act 1993. As at 1 April 2011, the Act is not in force.

20 The Credit Reporting Agencies Act 2010, s 24(1)(a) provides that "No credit reporting agency shall disclose any credit information for any purpose to any person unless the customer has given his consent to the disclosure." See Zulkifli Abd Rahman "Bill requiring credit-reporting agencies to obtain consent passed" (2010) The Star Online <http://thestar.com.my>.

The term "credit reporting business" as provided under the CRA 2010 means:[21]

> a business that involves the processing of credit information for the purpose of providing a credit report to another person, whether for profit, reward or otherwise, but shall not include the processing of credit information-
>
> (a) for the purpose of discharging regulatory functions or that is required or authorized by or under any law; or
>
> (b) by a credit rating agency.

Thus, all businesses which fall under this definition will be governed by the CRA 2010 and not by the PDP 2010. This specific exclusion of credit reporters from the ambit of the Act is harmful for data users whose information is collected by the credit reporters and sold to other parties. However, the Deputy Finance Minister Datuk Dr Awang Adek Hussin said that the activities of the credit-reporting agencies will also be checked through provisions under the Companies Act and the PDP 2010. The onus is on the credit-reporting agencies to prove that they have taken reasonable steps to provide the correct and up-to-date information in their database. This is to prevent problems of incorrect financial information on consumers through unverified sources.[22] In this sense, a consumer's data is protected from being intruded upon or altered as the consumer has the right to inspect and give consent as to whether the data is to be displayed or otherwise.

Further, following the public outcry over the Credit Tip-Off Service Sdn Bhd (CTOS) incident in 2007[23] involving the sale of personal and incorrect information about individuals, there were demands for legal protection without delay. The best way to overcome the problem of "selling and buying of information" is to have a code or regulation established under the PDP 2010 as is the practice in New Zealand,[24] and not a stand-alone law to govern the activities of the credit reporting business which directly relates to the security of personal data collected through its transactions. The question now is whether the CRA 2010 is adequate to protect consumer information from being misused and manipulated.

B Personal Data Protection Principles

It is a requirement under the PDP 2010 that a data user complies with all the data principles in processing personal data set out in Part II of the Act.[25] These principles are framed by reference to

---

21 Credit Reporting Agencies Act 2010, s 2.

22 See Rahman, above n 20.

23 See Izatun Shari "DPM: Govt may terminate CTOS' services" (2010) The Star Online <http://biz.thestar.com.my>.

24 The New Zealand Credit Reporting Privacy Code 2004 is established under the Privacy Act 1993.

25 Personal Data Protection Act 2010, s 5.

international instruments governing the protection of privacy and trans-border flows of personal data. The interrelationship of computers, freedom, privacy and trade has become the topic of concern among international organisations.[26] The seven principles are briefly discussed here.[27]

1 General principle

First, a data user shall not process personal data about an individual unless that individual has given consent to the processing of their personal data.[28] The personal data shall not, without the consent of the data subject, be disclosed except where the disclosure is for the purpose in connection with which it was collected or is directly related to data user's activity.[29]

2 Notice and Choice Principle

Second, s 7 prescribes that where a data user is required to give a written notice informing an individual ("data subject") that their personal data is being processed by or on behalf of the data user, the notice shall, amongst other things, include the purpose for which the personal data is being collected and whether it is obligatory or voluntary for the data subject to provide the personal data. The notice must be given at the earliest opportunity when the data subject is asked to supply personal data.

3 Disclosure Principle

The third point is that any disclosure made under the Act must be in compliance with s 8. Personal data shall not, without the consent of the data subject, be disclosed for any purpose other than the purpose which was initially disclosed at the time of collection or to any party other than third parties for whom the data subject has given permission.

4 Security Principle

Next, in dealing with personal data, security measures must be adopted in order to comply with Part II of the Act. Data users must take practical steps to ensure the security, reliability and integrity

---

26 Rosemary Jay *Data Protection: Law and Practice* (3rd ed, Sweet & Maxwell, London, 2007) at 6.

27 Various authors have addressed the personal data protection principles under the PDP 2010. Among them Khaw Lake Tee "Towards a personal data protection regime in Malaysia" (2002) JMCL 11, Abu Bakar Munir "Data Protection Law: Too little, too late?" (Public Lecture, Universiti Malaya, 4 August 2009), Ida Madieha Azmi "E-Commerce and privacy issues: An analysis of the Personal Data Protection Bill" (17th BILETA Annual Conference, Free University, Amsterdam, 5–6 April 2002) and Graham Greenleaf "Limitations of Malaysia's data protection Bill" (2010) 104 Privacy Laws and Business International Newsletter 1.

28 Personal Data Protection Act 2010, s 6.

29 Personal Data Protection Act 2010, s 6(2)(a)–(f).

of the personal data.[30] It is the duty of the data user to take all necessary steps to protect any loss, misuse, modification, unauthorised and accidental access or disclosure, alteration or destruction of personal data.

5 Retention Principle

Fifth, s 10 provides that the personal data processed cannot be kept longer than is necessary and the data user shall take all reasonable steps to destroy personal data that is no longer required. However, this provision does not specifically mention the life span of personal data.

6 Data Integrity Principle

Sixth, s 11 states that a data user must ensure that personal data is accurate, complete, not misleading and kept up to date, and related to the purpose for which it was collected. It is the duty of data user to guarantee the accuracy, completeness and correctness of the data collected.

7 Access Principle

The seventh principle is the "access principle"[31] which provides that a data subject shall be given access to, and be able to correct, amend or delete personal data whenever it is inaccurate. However, access or correction can be refused under the Act. Thus, in any processing and handling of personal data it is mandatory for the data user to observe all data protection principles and any contravention of the principles results in an offence committed by the data user.[32]

C Enforcement

The law will be meaningless without enforcement. The Act provides for a Personal Data Protection Commissioner who is appointed by the Minister and who has various functions[33] and powers[34] particularly in implementing and enforcing the law. The Commissioner is responsible for advising the Minister on the national policy for personal data protection and carrying out all relevant actions in exercising the administration of personal data as set out in the Act and directed by the

---

30 Personal Data Protection Act 2010, s 9.

31 Personal Data Protection Act 2010, s 12.

32 Personal Data Protection Act 2010, s 5(2). This section provides that on conviction, a data user shall be liable to a fine not exceeding 300,000 ringgit or to imprisonment for a term not exceeding two years, or both.

33 Personal Data Protection Act 2010, s 48. Among the functions are to advise the Minister on the national policy for personal data protection and related matters, to implement and enforce the personal data protection laws and to supervise compliance with the provisions of the Act.

34 Personal Data Protection Act 2010, s 49. The Commissioner has all power to do things necessary in connection with the performance of his functions under the Act.

Minister. However, despite the wide functions and powers granted to the Commissioner under the Act, the Commissioner is responsible and answerable to the Minister.[35]

The Commissioner has an administrative duty to decide whether there is a serious breach of personal data protection principles through complaints made by any person regarding an act or practice that contravenes the Act.[36] Upon receiving a complaint, an investigation will be carried out in accordance with s 105. The Commissioner may refuse an investigation if he or she is of the opinion that there has been no contravention of the provisions of the Act. On completion of the investigation, when the Commissioner is satisfied that contravention of the provisions of the Act occurred, an enforcement notice as provided under s 108 will be issued.

The Commissioner may later appoint an authorised officer to exercise the powers of enforcement under the Act. The decision specified in the enforcement notice can be challenged by filing a notice of appeal with the Appeal Tribunal. A decision of the Commissioner is not final. An aggrieved party may appeal to the Appeal Tribunal[37] whose decision is final and binding on the parties to the appeal.[38]

D Limitations[39]

1 Restriction to commercial transactions

Section 2 of the PDP 2010 provides that the Act applies only to a person who processes, who has control over, or who authorises the processing of personal data in respect of commercial transactions. This precludes the application of the Act to non-commercial affairs even though the information communicated in such transactions has just as much need for protection. Moreover, a clear exclusion of a credit reporting business as provided under the CRA 2010 does not offer any help to people whose banking information has been processed by credit reporting agencies.

---

35 Personal Data Protection Act 2010, s 59. In Graham Greenleaf "Limitations of Malaysia's data protection Bill" (2010) 104 Privacy Laws and Business International Newsletter 1, the author noted that this provision further underlines the Commissioner's lack of independence.

36 Personal Data Protection Act 2010, s 104.

37 Personal Data Protection Act 2010, s 93. The Appeal Tribunal shall consist of a Chairman and at least two other members of the Judicial and Legal Service of the Federation appointed by the Minister as stated under s 85 of the Act.

38 Personal Data Protection Act 2010, s 99 provides that the decision of the Appeal Tribunal on any matter shall be decided on a majority of members of the Appeal Tribunal and the decision is final. Section 100 provides that a decision given by the Appeal Tribunal may, by leave of the Sessions Court, be enforced in the same manner as a judgment or order to the same effect, and where leave is so given, judgment may be entered in terms of the decision.

39 Discussions on limitations of the PDP 2010 can also be found in Khaw Lake Tee "Towards a personal data protection regime in Malaysia" (2002) JMCL 11 and Greenleaf, above n 35.

2 *Government not bound*

The Act does not bind Federal Government and State Governments.[40] As far as data and personal information are concerned, governments are the biggest collectors and holders of personal data. Thus, the law must bind them if it is to prevent abuse and mishandling of personal data and protect information privacy. The non-application of the Act to public sectors has in fact made it less significant as it excludes a party that deals with personal data in most of its transactions.

3 *Commissioner's lack of independence*

Article 28 of the Directive provides that there must be an independent supervisory authority to enforce the law. Under the PDP 2010, a Personal Data Protection Commissioner appointed by the Minister has a range of powers.[41] Section 47(3) provides that the Commissioner is a body corporate having perpetual succession and a common seal. Obviously therefore, the Commissioner is not a natural person but an entity created by the law. The Minister may revoke the appointment, or the Commissioner may resign office by giving a written notice to the Minister.[42] This situation is irreconcilable with the Commissioner being a body corporate which has perpetual succession. The Commissioner is responsible to the Minister[43] and the Minister may give the Commissioner directions of a general character consistent with the provisions of the Act. Thus the position of the Commissioner under the PDP 2010 is not independent and fails to satisfy the EU adequacy requirement test.[44] This may affect the transfer of personal data though it may still take place provided that the originating party takes additional measures to ensure that data is adequately protected in Malaysia.[45] It is argued that the Commissioner should be answerable directly to Parliament in order to gain more independence in exercising his function under the Act. However, this argument is refuted on the basis that such a position would be a distortion from the established doctrine of separation of powers that is adopted by the Malaysian Constitution.[46]

---

40 Personal Data Protection Act 2010, s 3.

41 Personal Data Protection Act 2010, ss 47, 48 and 49.

42 Personal Data Protection Act 2010, ss 54(1) and 54(2).

43 Personal Data Protection Act 2010, s 59.

44 European Union Data Protection Directive 1995, art 25.

45 See Abu Bakar Munir "Malaysian Data Protection Law is Inadequate" (2010) <http://profabm.blogspot.com>.

46 In the Malaysian context, the governing bodies are the Executive, the Legislature and the Judiciary. Each body has specific powers that consist of enforcing making, interpreting and applying the law. Specific provisions on each of them are mentioned in the Constitution, arts 39–40 (the Executive), arts 73–79 (Legislative powers) and art 121 (the Judiciary). All of them are distinct from each other.

4 Personal data exclusions

Under s 45, the personal data protection principles will have no effect on personal data processed by an individual for personal, family, household affairs and recreational purposes. This broad exemption is in line with the main intention of the Act to protect personal data in commercial transactions only. Similarly, the processing of personal data for journalistic, literary and artistic purposes is exempted from the principles if the publication is in the public interest.

III Comparative Influences

A The United Kingdom and Hong Kong Data Protection Legislation

The personal data protection principles in the Hong Kong Ordinance are similar to PDP 2010. Briefly, a data user must: exercise lawful and fair collection of personal data, observe the accuracy and retention period of personal data, personal data used in the manner consented to by the data subject, apply security measures be open about the kinds of personal data they hold, and provide a right of access on the part of the data user to personal data.[47] As a result of the passing of the Ordinance, the Hong Kong Government is promoting good data protection practices in both its public and private sectors with the application of data protection principles and security measures for their implementation.

The UK Data Protection Act 1998 also contributed to the formulation of the PDP 2010. There are eight data protection principles spelt out in the 1998 Act. They are:

(1) the fair and lawful processing of personal data;

(2) the manner of obtaining personal data shall be specified and for lawful purposes;

(3) the adequacy and relevancy of personal data;

(4) the personal data shall be accurate and up-to-date;

(5) the retention period shall not be longer than necessary;

(6) the processing shall be in accordance with the rights of the data subject;

(7) appropriate measures to be taken against unlawful and accidental loss and destruction; and

(8) personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Looking to the nature of personal data which requires protection particularly in the electronic age, the heart of the law is the Data Protection Principles. As far as the PDP 2010 is concerned, it

47 Principles 1–6 of the Data Protection Principles, Hong Kong Personal Data (Privacy) Ordinance 1995.

contains all the relevant principles provided for in the United Kingdom and Hong Kong data protection legislation.

B International Guidelines

Besides the UK and Hong Kong data protection legislation, the international instruments referred to in the preparation of the PDP 2010 include the Organisation for Economic Cooperation and Development (OECD) Guidelines 1980 (the Guidelines), the Council of Europe Convention for the Protection of Individual with regard to Automatic Processing of Personal Data 1981 (the Convention), the EU Data Protection Directive 1995 (the Directive) and the APEC (Asia-Pacific Economic Cooperation) Privacy Framework 2004 (the Framework).

The protection of privacy and individual liberties and the improvement of the free flows of personal data are the two essential values addressed in the Guidelines. The core of the Guidelines consists of eight basic principles relating to the protection of privacy and individual liberties.[48] The principles highlighted in the Guidelines have been adopted by member countries in legislating data protection law and is reflected in the PDP 2010 as well.[49] However, it is interesting to note that the Guidelines apply to data held in both the public and private sectors. In contrast, the PDP 2010 states clearly that the Act has no application to the Federal and State Governments.

On the other hand, the Convention was promulgated with the idea that data protection was a human right concern and very much related to privacy. The central part of the Convention is Chapter II which sets out basic principles for data protection. It provides that personal data undergoing automatic processing shall be:[50]

(a) obtained and processed fairly and lawfully;

(b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

(d) accurate and, where necessary, kept up to date;

(e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

---

48 The Organisation for Economic Cooperation and Development (OECD) Guidelines 1980 [7]–[14].

49 They are the: Collection Limitation Principle, Data Quality Principle, Purpose Specification Principle, Use Limitation Principle, Security Safeguards Principle, Openness Principle, Individual Participation Principle, and Accountability Principle.

50 Europe Convention for the Protection of Individual with regard to Automatic Processing of Personal Data 1981, art 5.

Thus, the aim is the fulfilment of two fundamental legal standards. First, the information should be correct, relevant and not excessive in relation to its purpose. Second, its use including gathering, storage and dissemination should likewise be within the purpose for which it is obtained. Interestingly, the Convention has many elements in common with the Guidelines. The essential difference between the two documents is that the Convention is intended to be adopted as a binding instrument by states. Unlike the Guidelines, the Convention requires that signatories modify their national laws to meet its specifications.[51]

In addition, the Directive aims to protect personal information about individuals and preventf any restrictions on the free flow of personal information between member states and sets the benchmark for the national law of each member state.[52] This will harmonise the law on data protection throughout the EU. The Directive outlines various principles upon which data collection, use and access may proceed.[53]

Article 25 of the Directive provides that no personal data may be transferred to a third country unless the "third country in question ensures an adequate level of protection". The Directive does not require that the third country must have data protection legislation before it can be considered to provide adequate protection.[54]

Thus, a country with no protection or no adequate protection for personal data may face difficulty in the flow of information from EU member states which will definitely impact on the development of commerce and trade. This requirement of the EU Directive has prompted the Malaysian Government to introduce data protection legislation that will meet the requirements of the Directive.

The last model is the APEC Privacy Framework 2004, which is the most significant international privacy instrument since the EU privacy Directive of the mid-1990s. The role of the APEC is to balance and promote effective information privacy protection and the free flow of

---

51 David M Cooper "Transborder Data Flow and the Protection of Privacy: The Harmonization of Data Protection Law" (1984) 8 Fletcher F 335 at 348.

52 European Union Data Protection Directive 1995, art 1.

53 European Union Data Protection Directive 1995, art 6 provides that personal data must be processed fairly and lawfully; collected for specified, explicit and legitimate purposes; adequate, relevant and not excessive in relation to the purposes for which the data was collected; accurate and kept up to date; kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

54 There are six basic principles suggested in order to assess the adequacy of protection. These include the purpose limitation; the data quality and proportionality; the transparency; the security; the right of access, rectification and opposition; and restriction on onward transfer.

information in the Asian Pacific region in order to ensure the growth of electronic commerce.[55] The Framework is intended to provide clear guidance and direction to businesses in APEC economies on common privacy issues and the impact of privacy issues upon the way legitimate businesses are conducted. Thus, the primary aim of the Framework is to promote the growth of e-commerce rather than to address human rights and dignity.[56] While the Framework is based on the core value of the OECD Guidelines, the information privacy principles set out in the Framework do not much differ from the Guidelines.[57]

IV Critique

The passing of the much awaited PDP Act 2010 follows a great effort by the government in relation to the processing and use of personal data. Malaysia is the first ASEAN country to have a specific law on data protection. It is hoped that it will become a model for other ASEAN countries to develop such law. However, a close analysis of the Act suggests that there is room for improvement.

The obvious shortcoming of the PDP Act 2010 is the definition of personal data. Why it is confined to specified commercial transactions? Why not make it more general to cover all purposes, as in other countries? What protection is there for personal data of a non-commercial character? These are the questions that become the central concerns in order to improve the Act so that it will cover all circumstances in which personal data is collected and processed. It is interesting to note that the Act applies only to commercial transactions while the precedents that inspired the Act are generally applicable to all purposes. Little information is protected while this definitional limitation remains.

The non-applicability of the PDP Act 2010 to Federal and State governments, as highlighted by s 3, raises a question as to different standards governing data of public and private bodies. What kind of protection is available if the data user is dealing with the government in regard to the same data? The fact that the Act does not bind the government will result in double standards in the treatment of the same type of data. Interestingly, this is the only Act on data protection that excludes

---

55 The objective of APEC Privacy Framework 2004 is mentioned in Johanna G Tan "A Comparative Study of the APEC Privacy Framework – A New Voice in the Data Protection Dialogue?" (2008) 3 Asian Journal of Comparative Law article 7 at 16.

56 See APEC Privacy Framework [1] and [6] of the Preamble.

57 The principles are (1) preventing harm; (2) notice; (3) collection limitation; (4) uses of personal information; (5) choice; (6) integrity of personal information; (7) security safeguard; (8) access and correction; and (9) accountability.

its applicability to the public sector.[58] By having different standards, full protection over personal data is hard to achieve. However, according to the Information, Communications, Culture and Arts Minister Datuk Seri Dr Rais Yatim, the reason why the Act binds only the private sector is because safeguards were already in place to take care of government channels but there were insufficient regulations on the use of personal data in the hands of irresponsible people. He said that the government already possesses the relevant authorities and legal controls and parameters, such as the Official Secrets Act, and law pertaining to creditors.[59]

The Official Secrets Act 1972 (the OSA) is the law that protects the government's official secrets whereas the PDP 2010 aims at protecting personal data in commercial transactions. Section 2 of the OSA defines official secret as official document, information and material as may be classified as "Top Secret", "Secret", "Confidential" or "Restricted" by a Minister or public officials. The publication of such information which endangers national security will be subjected to stiff fines and imprisonment.[60] However, the OSA contains no provisions providing protection of personal data processed without consent as intended by the PDP 2010. These two laws do not have the same objective, therefore the exclusion of public sector from the purview of the PDP 2010 on the basis that protection is provided by the Official Secrets Act does not address the problem of different standards in dealing with personal data and the absence of protection for individuals whose personal data is held by government.

Though data should be protected as part of an individual's right to privacy, this Act is not privacy driven as it discusses provisions on personal data protection in relatively few sections.[61] The remaining provisions provide and explain the administration and maintenance of the system of handling of personal data. The ultimate end of protection – remedy for individuals – is absent from the Act. There is no provision in the Act for compensation for an individual whose data has been

---

58 Other legislation provides for the protection of data in both public and private sectors. South Korea, for example, has two separate laws. The Act on the Promotion of Information and Communications Network Utilization and Information Protection 1999 was enacted to provide guidelines for personal information in the private sector whereas the Act on the Protection of Personal Information Maintained by Public Agencies 1994 was introduced to govern the personal information protection in public sector. Refer to Chang-Boem Yi and Ki-Jin Ok "Korea's personal information protection laws" (2003) PLPR 8.

59 Yeng Ai Chun "Personal Data Protection: Govt has own mechanism" The Star Online (2009) <http://thestar.com.my>. Laws pertaining to creditors include the Pawnbroker Act 1972, the Hire Purchase Act 1967 and the Moneylender Act 1951.

60 See Official Secrets Act 1972, ss 3, 4 and 5. Under the Communication and Multimedia Act 1998, it is an offence to make, create or transmit any communication with the intention to abuse or harass another person using network facilities or services. Again, nothing in the Act provides protection for the abuse of personal data.

61 The Personal Data Protection Act 2010 points out personal data protection principles in ss 5–12 and rights of data subjects in ss 30–44.

misused. Though correction of inaccurate information is granted under the Act,[62] the main focus of the Act is on sanctions for breach.[63] This might provide some deterrence against breach, but does not compensate the victim. Due consideration should be given to this matter to ensure fair treatment of data subjects because if the data user contravenes the Act, the fine or imprisonment that may be imposed may be little consolation to the data subject whose data has been processed or released without consent.

The PDP 2010 should provide specifically for private remedies such as damages in terms of monetary compensation and injunctions to the data subjects affected as a result of a breach of privacy. This would encourage compliance and restrain further invasion. This is in line with the international precedents which provide compensation for individuals who have suffered distress caused by any contravention by the data controller.[64] In the UK, while there are no guidelines as to the appropriate level of compensation for a claim under the Act, the judge has discretion and would have to take into consideration many factors including the seriousness of the breach and the effect upon the claimant in assessing damages for distress.[65] For example in the case of *Jacklyn Adeniji v Newham Council*,[66] the High Court awarded the claimant £5,000 in damages and £50,000 for legal costs for breach under the Data Protection Act 1998 and the Human Rights Act 1998 after using her photograph without permission. In *Campbell v Mirror Group Newspapers*, [67] monetary compensation of £3,500 was awarded for both breach of confidence and under the DPA 1998.[68]

The next point of critique is the position of the Commissioner, whose position is a body corporate placed under the Ministry. This shows a lack of independence in the execution of its function. Looking to the nature of the duties and powers assigned by the Act, the Commissioner should be independent and should be made accountable directly to the Parliament. As the Commissioner holds a very important position in relation to personal data protection issues, greater accountability is needed in discharging his duties.

In short, there are the flaws that should be addressed if Malaysia is to have a comprehensive protection system for processing and handling of personal data.

---

62 Personal Data Protection Act 2010, s 34.

63 Ibid, 5(2).

64 This is provided under the Data Protection Act 1998 (UK), s 13 and of the Hong Kong Personal Data (Privacy) Ordinance 1995, s 66.

65 See Information Commissioner "Data Protection Act Claiming Compensation" <www.ico.gov.uk>.

66 *Jacklyn Adeniji v Newham Council* October 2001, High Court. This case was settled out of court, therefore no reported decision is available. For more information see Ibrahim Hassan "Data Protection Update 2002" (2002) <www.actnow.org.uk>.

67 *Campbell v Mirror Group Newspapers* [2004] UKHL 22, [2004] 2 All ER 995.

68 See Ibrahim Hassan, above n 66.

V Conclusion

More than a decade of waiting ended with the passing of the PDP 2010. It is the first step taken by the government to protect the private handling of personal data for commercial purposes. Despite its deficiencies, the PDP 2010 is now law and its implementation and enforcement will be the test of its success.

The Act indicates that the government is serious in dealing with an aspect of privacy protection, for instance personal data, despite its narrow and limited application. The preamble itself indicates the Act is confined to commercial transactions. This limited scope deviates from best international practice as well as from the two jurisdictions that Malaysia referred to when preparing the PDP 2010. It is believed that political expediency is one of the reasons why the PDP 2010 was passed as it is.

The passing of the Act in a way becomes a platform to recognise the right to privacy or at least personal privacy, however it is not that simple as the Malaysian Constitution and the courts[69] have not recognised privacy rights. It is clear from the reading of the Act that privacy protection is not the motive behind the introduction of the Act. In fact, the legislation is a set of rules which provides protection of commercial interests in data and enables Malaysia to participate internationally particularly in cases of trans-border flow of personal data.[70]

It seems the Act was not intended to recognise the right to privacy, but rather the seriousness of the government in handling, processing and treating personal data is evidenced through the passing of the Act. The Act's effectiveness to fulfil the overall intention of data protection law might be achieved if the phrase "commercial transactions" is removed so the law can cover all purposes. The Act must also bind both public and private sectors to ensure fair treatment of personal data. Last but not least, a clear provision on compensation or injunction rights to the person who suffered damage must be included as part of remedies available. It is hoped that the Act will become a stepping-stone to better protection in the future.

---

69 The court in *Ultra Dimension Sdn Bhd v Kook Wei Kuan* [2004] 5 CLJ 285 (HC), held that the right to privacy is not recognised under the Malaysian law.

70 This is in line with the European Union Data Protection Directive 1995, art 25 that requires an adequate level of protection before personal data may be transferred to a third country.