2011 International Conference on Sociality and Economics Development
IPEDR vol.10 (2011) © (2011) IACSIT Press, Singapore

Personal Data Protection in the Business of Higher Education: Malaysian Law

Kamal Halili Hassan[1]

Faculty of Law,
Universiti Kebangsaan Malaysia

Abstract. This paper discusses the legal application of personal data protection in higher education in Malaysia. The Personal Data Protection Act which was passed by the Malaysia Parliament in 2010 is a new statute and many people affected by the Act are still unclear about its provisions. The Act however has until to date not been enforced yet. In this paper, the data protection law is discussed in the context of higher education in Malaysia. A lot of personal data are kept in universities and colleges. The author discusses the salient features of the Acts such as the categories of personal data, the responsibilities of data users and the rights of data subject.

Key words: Data protection, Malaysian law, higher education, privacy

1. Introduction

Higher education, either in public or private sector, nowadays has gone beyond the traditional way of delivering its services. In the era of globalisation, usage of modern technology such as the internet has become a norm in university's administration and dispensing of knowledge. In this context, universities all over the world has embraced this modern phenomenon where teaching has been made via on-line, syllabus stored in disc and web, lecturers setting up blogs, personal and academic data stored and university administration are done electronically. Some universitites operate their academic teaching largely via on-line. One prominent feature of universites is keeping and maintaning data, be it for personal or group purposes. In the world of knowledge economy, data is important as it is a record of individual history, knowledge and intellectual achievement. The law must protect data from unauthorised disclosure. The protection of data creates a sense of confidence and intergerity. This paper discusses the legal provisions that protect personal data. To that end, the Malaysian Personal Data Protection (MPDP) Act 2010 is used as a point of reference. The discussion of this part is divided into three parts: (i) features of a university; (ii) salient features of MPDP Act 2010 and (iii) the rights of the data subject under the MPDP Act 2010. It mus be borne in mind that the 2010 Act only deals with personal data, not data owned by organisation.

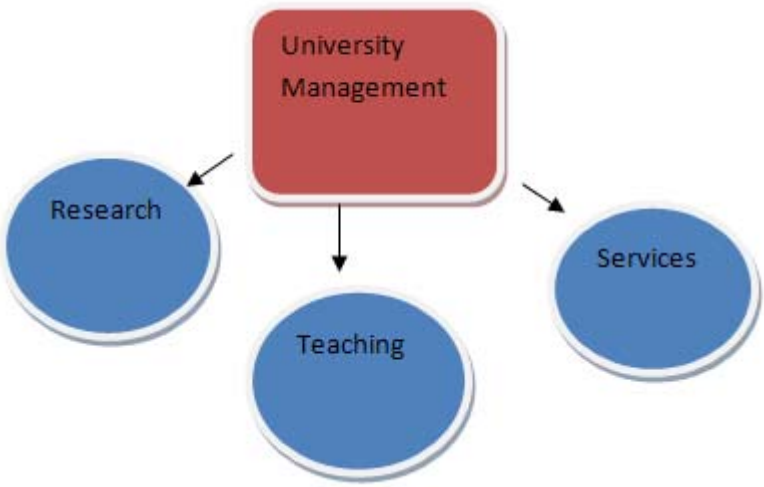
2. Personal data and University management

The academic activities of a university are basically of three fold: education, research and services. Education here refers to the teaching and learning of students at both the undergraduate and postgraduate levels. The mode of teaching is carried out by way of conventional and modern methods. The latter uses a lot of electronically means especially the internet. Various online materials are stored and transmitted electronically by universities to students and these materials are considered as data. Research carried out by the academicians is the main activity in universities especially the ivy league universities or public universities. Research carries a lot of data which can be related to the researchers. Data emanated from research is usually kept confidential by the universities and in some cases those data are protected under

[1] Corresponding author Tel.: 603-89216355; fax: 603-89253217
E-mail address: k.halili@ukm.my

intellectual property law. The services rendered by university and its academic staff also contained a lot of data. In medical faculties and university hospital, a huge volume of data are kept either referring to the staff or patients. All these data refer to individual historical background, illnesses and insurance. Beside all those three main activities, E-university also refers to its administration. The university administration keeps data of its individual staff either electronically or manually. Besides staff data, university also keeps students' data. Those data relates to individual history of education, addresses, examination results, illnesses, family, scholarship parents' salary and expenditure. Currently with modern technology, staff and students' data are stored by electronic means. In academia, personal data is used widely, in fact academic staff are very proud in displaying their biodata and it can be easily found in either their personal or university web site. The act of university staff displaying their biodata is made voluntary to inform the public of their area of expertise and achievement. The act is bona fide and it will not cause any problem as long as it is used for good and lawful purposes. However, the administration who keeps and administers the staff and students's data owe a legal duty not to disclose it to un- authorised party.

The graph that follows illustrates the features of a university.



3. Universities/Colleges in Malaysia

Universities in Malaysia are either public or private, but the latter far outnumber the former. There are 22 public universities in Malaysia. There are more than 400 universities/colleges that operate on e-teaching substantially and some using the traditional mode and some of mixed or blended modes. The public university has been traditionally strong in teaching the conventional way. The academic staff, especially among the professors, have been used to teach students by the face-to-face method. However, even in public universities now academic staff are advised to adopt and adapt to e-teaching. Teaching materials are now uploaded and stored in computers and assignments are submitted via emails. It is submitted that some private universities are going to farther extent in teaching via the electronic means. Universities such as the open universities and Universiti Tun Razak are considered as the pioneers in virtual education.

4. Right to Privacy

Data protection law has already been widely enforced in developed economies (Schwartz, 1995, Cate 1995). In some countries, the law on data protection is called privacy law (Azmi 2002,). It is argued that the meaning of privacy is wider than data protection which is more direct. There have been many definitions of 'privacy' put forward by writers but the definitions have never been very clear, to the extent that the Calcutt Committee in the UK said. "nowhere have we found a wholly satisfactory statutory definition of privacy" (Munir and Yasin 2002). However, the Committee defines privacy as; "the right of the individual to be protected against intrusion into his personal life or affairs. Or those of his family, by direct physical means or by publication of information". The Common Law and the International Human Right documents recognise the right of the individuals to privacy. The right to privacy has been expressed as a fundamantal human right. Article 12 of the United Nations Universal Declaration of Human Rights adopted in 1948, proclaims that:

"no one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".

5. Salient features of Malaysian Personal Data Protection Act 2010

The MPDP Act 2010 is long overdue. For many years, the law on privacy is not very clear in Malaysia to the extent that some quarters are of the opinion that there is no such law in this country. In the late 2009, the Malaysian Parliament debated the bill (Munir and Yasin 2002, 2010). In this part, the author will discuss some salient features of the Act. This Act protects personal data of an individual (Jawahitha et al 2007). The Act has todate has not been enforced yet by the Government. However, it is wise for Malaysian to be made known of the salient features of the Act prior to its enforcement. What is a personal data? Personal data refers to data of any individual or person or under the Act is called a 'data subject'. Consequently it excludes companies or corporations. But if it is the 'data user', that is the persons who keeps or operates the data, persons here refer to individual and corporations.

Section 4 of the Act defines personal data as any information in respect of commercial transactions which

(a) is being processed wholly or partly by means of equipment operating automatically in response to transactions 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 relevent filing system or with the intention that it should form part of a relevant filing system.

- It looks that the Act only applies to data related to commercial transaction. Commercial transactions in this context is defined as 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 insurance. A question arises whether e-university falls under 'commercial transaction'? It is submitted that e-university fall under such category. A university activities involve the supply of services that is teaching and learning of students who pay fees. It is a commercial transaction that involve issues of profit and loss. For private universities in Malaysia, making profit is the primary factor of their existence and for that matter, they are clearly governed by the 2010 Act.
- The Act, like any other legislation, also concern issues of jurisdictional application. Basically, if the data users and subjects are Malaysian citizens, the legislation will automatically covers them. Jurisdictional application in this context refers to the person and the place of equipement that processes the data. Section 2(2) privides that sub-s (1):
- This act shall apply to aperson in respect of a personal data:
  - *If the person is established in Malaysia and the personal data is processed, whether or not in the context of the establishment, by that person or any other person employed or engaged by that establishment; or*
  - *If 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.*
- Must the data be operated by an equipment automatically? What if it is manually done? Section 4 rcovers two situations, one that refers to processes by electronic means and second, by a relevant filing system. The first way is clear, the data must be processed by an equipment automatically, for example by a personal computer. The second way is a bit unclear. According to Bakar Munir and Siti Hajar (2010), 'relevant filing system' includes manual information in a filing system. This is based on section 4 which 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 the criteria relating to individuals, in such a way that specific information relating to particular individual is readily*

accesible'.

- The definition emphasises on the term 'set' which means that the the data must be of some structured of data stroing or collection. What is important is that there must be some specific information relating to a particular individual to be readily accesible. 'Readily accesible' would be that the data could be accessed or retrieved without any great obstacle, whether by electronic or manual way. Again, relevant filing system here denotes also to manual data which is structured and can be reached.
- The data must related to an individual directly or indirectly. There is no problem to understand the data situation of direct relation to a particular individual. But how is indirect relation fit to a protected data under this law? Indirect relations here means that in any given situtaion such as in business matters or entities, when the particulars of such business refers to that individual then the data is said to refer to that person. Consequently, data about him will attract protecion under the legislation. The personal data of a person must be able to be identified or identifiable as a known person. In other words, his or her identity must be easily identified identifiable. A common name will not attract legal personal data protection it it fails to be linked to any clear identity of an individual. However, if two or more separates or distinct information combine together can point to a particular individual then that information will be a personal data. For example, if some information in computers and some in manual file are combined together and are that information are identified as an information of an individual, therefore that qualifies as personal data under the legislation.
- The MPDP Act applies to any person (data user) who processes data. Section 4 defines 'processing' as:

> - '*Collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including the organisation, adaptation or alcateration or personal data, the retrieval, consultaion or use of personal data, the disclosure of personal data by transmission, transfer, dissemination or otherwise making available, or the allignment, combination, correction, erasure or destruction of personal data'.*

- Jurisdictional application is important to determine who will be subject to this legislation. The primary issue is whether the person concerned is a Malaysian or not; and the place the equipment is used. Section 2(2) provides that subject to sub-s (1), this Actshall apply to a person in respect of personal data: (a) if the person is established in Malaysia and the personal data is processsed, whether or not within that establishment, by that person or any other person employed or engaged by that establishment; or (b) if 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.
- There is an exception provided by the Act where the Federal and State Government are exempted from the governance of the Act. This exception has far reaching ramification as these governments keep many personal data. Government hospitals, for example, are exempted from the Act as they are governed by the Ministry of Health, which is a federal government agency. So do other agencies which keep many personal data such the Immigration Department and National Registration Department, exempted from the Act. However, the statutory bodies are not exempted as legally speaking they are neither under the federal or state governmment. The case in hand is the public universities, all of them are established under a special legislation. Although their funding and direction are very much governed by the federal government, legally they are not federal government agency, thus they are not exempted under this Act.

5.1. Data Protection Principles

- General principle - Consent of the data subject is the fundamental element. He or she must give his or her consent before any personal data about him can be divulged by the data user.
- Notice and choice principle - If the data subject is processing the personal data of the data subject, he must give notice to the the data subject. This is to inform the data subject of such processes. The data subject must be given a chioce to limit the extent of his personal data.
- Disclosure principle - Data cannot be disclosed to any party without the consent of the data subject other than for its original prupose.

- Security principle - Data user must during processing data ensure that data is not lost, misuse. modiifed, destructed or accidentalkly access. This is to ensure that data of a person is secured.
- Retention principle - The duration of keeping data must be observed by the data user. Data should not be kept longer than necessary.
- Data intergrity principle - Personal data must be accurate, complete, not misleading and kept up-to-date.
- Acess principle - Opportunity must be given to the data subject to access his personal data and to be able to correct it.

University administrative staff must ensure that all the above principles are adhered to in their daily adminsitration. It is suggested that a manual or guideline pertaining to the above duites be prepared for easy reference and application for the university administration.

5.2. Rights of the Data Subject

The MPDP 2010 Act lays down the following rights of data subject:

- s.32: Staff or students shall be given the right of access to their personal data,
- s. 36: Staff or students shall have the right to correct their personal data,
- s.40: Staff or students shall the right to prevent the collection of data that is likely to cause damage or distress,
- s. 41: Staff or students shall have the right in relation to automated decision-takings,
- s. 42: Staff or students shall have the right to non disclosure of personal data,
- s.43: Staff or students shall have the right to withdraw consent for purposes of usage of data,
- s. 44: Staff or students shall have the right to erase personal data that is no longer required.

University management must ensure that the data subject (staff and students) are given the above rights.

6. References:

[1] Abu Bakar Munir & Siti Hajar Mohd Yasin, "*Data Privacy and Data Protection",* Sweet and Maxwell Asia: Petaling Jaya, 2002.

[2] Abu Bakar Munir & Siti Hajar Mohd Yasin, "The Personal Data Protection Bill 2009" [2010] 1 *MLJ* cxix.

[3] Fred H.Cate, The EU Data Protection Directive, Information Privacy, and the Public Interest, 80, *Iowa L. Rev*. 431, (1994-95).

[4] Ida Madieha Azmi, "E-Commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill", *International Review of Law Computers & Technology,* Vol. 16, No.3, 2002, p 317-330.

[5] Paul, M Schwartz, "European Data Protection Law and Restrictions on International Data Flows", 80, *Iowa L. Rev*. 471, (1994-95).

[6] S Jawahitha, M.Ishak & M. Mazahir, E-Data Privacy and the Personal Data Protection Bill in Malaysia, *Journal of Applied Science*, 2007.