Manuscript Submitted	5.10.2023
Accepted	28.11.2023
Published	31.12.2023

Data Privacy Practices of Private Higher Education Institutions in Malaysia: A Preliminary Study

Surianom Miskam, Nawal Sholehuddin, Farah Mohd Shahwahid, Tuan Nurhafiza Raja Abdul Aziz & Naqibah Mansor

Faculty of Syariah and Law
Universiti Islam Selangor (UIS)
surianom@kuis.edu.my, nawal@kuis.edu.my, farahms@kuis.edu.my, tuan.nurhafiza@kuis.edu.my, mansornaqibah7@gmail.com

Abstract

Private higher education institutions as data users are subjected to the requirements of the Personal Data Protection Act 2010 (PDPA). These institutions process employee data as well as data of potential students, active students and alumni. They also deal with data of third parties such as vendors, visitors and contractors. Ten years after the coming into effect of the PDPA in 2013, the education sector has yet to develop their personal data protection code of practice as required by the Act. The General Code of Practice (CoP) of Personal Data Protection was introduced in December 2022 with the objective to provide guidelines to the Class of Data Users who have not prepared a Code of Practice and there is no data user forum to develop the relevant Code of Practice for the Class of Data Users. As the General CoP is legally binding, it is an offence punishable under the Act for any data user for failure to comply with any provision of this General CoP. As data users, private higher education institutions need to introduce certain mechanisms to adhere to the requirements such as privacy policy and procedure. This paper aims to compare the data privacy practices of private higher education institutions in Malaysia in order to determine to what extent the law has been complied with. Being a qualitative study, this paper applies content analysis technique. Data privacy policies of four private higher education institutions in Malaysia were examined to attain the objective. The four private higher education institutions are Universiti Tenaga Nasional (UNITEN), Universiti Teknologi PETRONAS (UTP), Taylor's University and University of Nottingham Malaysia. The data privacy policies of the four institutions are accessible on the official website of the institutions. The study indicates that in the absence of a personal data protection code of practice for the education sector as a guideline, the data privacy practices of the institutions vary from one to another. While some of the privacy policies contain provisions which are general in nature which may lead to confusion to the data subjects, the data privacy policies show that the four institutions have, to a certain extent, complied with the requirements of the PDPA in general.

***Keywords*:** *Data privacy, private higher education institutions, personal data protection, Code of Practice, data user.*

1. Introduction

Private higher education institutions as data users are subjected to the provisions of the Personal Data Protection Act 2010 (PDPA). These institutions process employee data as well as data of potential students, active students and alumni. They also deal with data of third parties such as vendors, visitors and contractors. Those categories of data contain personal data of individual data subjects that fall under the ambit of the PDPA. Private higher education institutions need to introduce certain

mechanisms to adhere to the requirements such as privacy policy and procedure. The institutions deal with a seemingly endless supply of data, a substantial portion of which consists of personal data including sensitive information. The institutions are increasingly focusing their activities on information and communication technology thus increasing the risk of exposing personal data to parties with malicious intention (Fernandes et. al., 2022).

In order to regulate data processing activities, the law provides that a code of practice may be prepared by a relevant data user forum either on its own initiatives or upon the request by the Commissioner of Personal Data Protection. The forum shall take into consideration certain matters among others, the purpose for the processing of personal data and the views of the data subjects or groups representing data subjects. The forum should also consider the views of the relevant regulatory authorities, to which the data user is subject to, and that the code offers an adequate level of protection for the personal data.

However, ten years after the coming into effect of the PDPA back in 2013, the education sector has yet to develop their personal data protection code of practice as required by the PDPA. On this point, the General Code of Practice (CoP) of Personal Data Protection was introduced in December 2022 with the objective to provide guidelines to the Class of Data Users who have not prepared a Code of Practice and there is no data user forum to develop the relevant Code of Practice for the Class of Data Users. By having its legally binding effect, any data user who fails to comply with any provision of this General CoP commits an offence which is punishable under the PDPA. In the absence of code practice for the education sector, the private higher education institutions need to introduce privacy policy to adhere to the requirements of the PDPA.

The objective of this paper is to compare the data privacy practices of private higher education institutions in Malaysia. This paper is structured as follows: Part 2 provides a summary of past studies by reviewing concepts and definitions of terms relevant to data privacy. Part 3 provides an overview of the data privacy law in Malaysia. Part 4 discusses the seven principles of personal data protection while Part 5 identifies the rights of a data user as enshrined in the Act. Part 6 describes the methodology applied in this study. Part 7 discusses the findings of the study. Finally, Part 8 concludes the paper by providing recommendations for future research.

2. Data privacy: Concepts and Definitions

Privacy is the claim of an individual to decide what information about himself or herself should be made known to others (Westin, 2003). Conceptualising privacy can be attained by discussing six general headings namely the right to be alone, limited access to the self, secrecy, control over personal information, personhood and control over or limited access to one's intimate relationship (Ataei et al., 2018). Privacy has become a major legal issue in recent years, prompted by constant improvement in technology and with the advent of big data and cloud computing. It follows that legal issues around information privacy have become more complex as data is transferred across jurisdictions (Pelteret & Ophoff, 2016).

Personal data is a set of data relevant to and used to identify a certain individual (Addae et al., 2017). Personal data refers to the information of an identifiable individual in commercial transactions whether or not it directly or indirectly relates to the data subject (Noor Sureani et al., 2021). An identifiable individual who can be identified whether directly or indirectly, specifically by reference to an identifier such as name, identification number, location, an online identifier or factors specific to the physical, psychological, genetic, mental economic, social or cultural identity of that individual (Sudarwanto & Kharisma, 2022). Information of personal data is a part of the privacy concept, thus the right to choose whether or not to disclose or provide personal information to other parties is the right of that individual (Sudarwanto and Kharisma, 2022).

The basic principle of personal data processing requires that any activities of personal data processing should be lawful, fair, appropriate, relevant and limited to what is necessary for the purpose for which they are processed and up to date (Katulic et al., 2022).

3. Data Privacy Law in Malaysia

Data privacy law in Malaysia is governed by the Personal Data Protection Act 2010 (PDPA) that came into effect in 2013. The legislation was passed to govern the processing of personal data in commercial transactions and all matters connected or incidental to consumers' personal data (Leng et al., (2021). Processing as defined under section 4 means "collecting, recording, holding, or storing the personal data or carrying out any operation or set of operation on the personal data including the (a) organisation, 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."

Pursuant to this Act, several subsidiary legislations have been passed to ensure the implementation of the Act, namely the Personal Data Protection (Class of Data Users) Order 2013, Personal Data Protection (Class of Data Users) Amendment 2013, Personal Data Protection (Compounding of Offences) Regulations 2013, Personal Data Protection (Registration of Data User) Regulations 2013, Personal Data Protection (Fees) Regulations 2013 Personal Data Protection Regulations 2013 and Personal Data Protection Standard 2013.

The PDPA is applicable to a data user which comes under the definition 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 a person who has control over or authorizes the processing of any personal data, but does include a data processor." On this note, private higher education institutions are categorized as data users by virtue of Para 7 (a) Schedule of Personal Data Protection (Class of Data User) Order 2013. Para 7 stipulates that entities under the education sector include private higher education institutions registered under the Private Higher Education Institution Act 1996.

The PDPA is only applicable to data that falls under the definition of 'personal data' as defined in section 4. The provision provides that personal data means "any information in respect of commercial transactions, which (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user which includes any sensitive personal data and expression of views about the data subject, but does not include any information that is processed by a credit reporting agency under the Credit Reporting Agencies Act 2010."

In this regard, commercial transactions refer to any transaction of a commercial nature, whether in performance of a contractual obligation or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but this definition excludes a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act 2010.

4. Personal Data Protection Principles

Compliance with the PDPA is guided by the seven data protection principles provided under section 5 (Sudarwanto and Kharisma, 2022). Each principle is defined as follows:

4.1 The General Principle

The general principle under section 6 of the PDPA deals with two types of personal data i.e. personal data other than sensitive personal data and sensitive personal data. Section 6 (1) stipulates that "a data user shall not, (a) in the case of personal data other than sensitive personal data, process personal data about a data subject unless the data subject has given his consent to the processing of the personal data; or in the case of sensitive personal data, process sensitive data about a data subject except in accordance with the provisions of section 40." For example, in situations when the processing is required for the purpose of any legal actions or for the administration of justice.

4.2 The Notice and Choice Principle

The notice and choice principle section 7 provides that "a data user shall by written notice inform a data subject (a) that the personal data of the data 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 purpose 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 request access to and to request correction of the personal data and how to contact the 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 iti 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." Section 7 (3) further provides that the written notice shall be provided in the national and English languages and the data user must be provided with a clear and readily accessible mechanism in exercising his choice.

4.3 The Disclosure Principle

The disclosure principle under section 8 must be read together with section 39 which deals with the extent of disclosure of personal data. Section 8 states that "no personal data shall, without the consent of the data subject, be disclosed (i) for any purpose other than the purpose for which the personal data was to be disclosed at the time of collection of the personal data; or (b) a purpose directly related to the purpose referred to in subparagraph (i); or to any party other than a third party of the class of third parties as specified in paragraph 7 (1)(e)."

However, section 39 provides certain exceptions where personal data may be disclosed without the data subject giving consent. The exceptions include that following circumstances: "(a) the data subject has given his consent to the disclosure; (b) the disclosure is necessary for the purpose of preventing or detecting a crime, or was required or authorised by or under any law or by the order of the court; (c) the data user acted in the reasonable belief that he had in law the right to disclose the personal data to the other person; (f) the data user acted in the reasonable belief that he would have had the consent of the data subject if the data subject had known of the disclosing of the personal data and the circumstances of such disclosure; or (e) the disclosure was justified as being in the public interest in circumstances as determined by the Minister."

4.4 The Security Principle

The security principle is dealt with under section 9 of PDPA. Section 9 provides that "a data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction by having regard (a) to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction; (b) to the place or location where the personal data is stored; (c) to any security measured incorporated into any equipment i which the personal data is stored; (d) to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and (f) to the measures taken for ensuring the secure transfer of the personal data."

In circumstances where data processing is carried out by a data processor, section 9 (2) requires the data user to take measures to ensure that the data processor provides adequate guarantees in respect of security measures regulating the processing of personal data, and takes reasonable measures to ensure compliance to proposed measures. In complying with the principle, the measures taken by the data user would vary depending on the industry the data user is operating its commercial activities as well as the type of personal data that is being processed. For the banking, insurance, health and communication industries which deal with sensitive, confidential and valuable personal data on a daily basis, data users are required to take high level security measures to safeguard the personal data in order for them to adhere to the requirements of security principle.

4.5 The Retention Principle

The retention principle under section 10 states that "the personal data processed shall not be kept longer than is necessary for the fulfilment of that purpose." Therefore, it is the obligation of the data user to dispose or permanently delete the personal data once the purpose of processing the data has been achieved. The phrase 'shall not be kept' in that section shows that it is mandatory for the data user to dispose of the data when it is no longer needed for its purpose. However, the PDPA does not mention nor determine the period for which the data user must carry out the deletion or how to determine when to dispose of the data.

4.6 The Data Integrity Principle

Section 11 explains the data integrity principle that stipulates that "a data user shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed."

4.7 The Access Principle

The access principle provides that "any data subject shall be given access to his personal data held by a data user and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access is refused under this Act. "collected and processed by the data user." In case when the personal data is inaccurate, the data subject must be allowed to exercise his right to correct the data to give effect to section 12.

5. Right of data subject

Data subject under section 4 refers to an individual who is the subject of the personal data. The PDPA further expressly stipulates that a data subject has certain statutory rights under the law. The six rights are the right to be informed (section 30 (1)), the right of access to personal data (section 31), the right to correct personal data (section 34), the right to withdraw consent (section 38), the right to prevent processing which is likely to cause damage or distress (section 32) and the right to prevent processing for direct marketing purposes (section 43).

6. Methodology

Four private higher education institutions in Malaysia were selected for this preliminary study. The selected private higher education institutions are Universiti Tenaga Nasional (UNITEN), Universiti Teknologi PETRONAS (UTP), Taylor's University and University of Nottingham Malaysia. The selection was made based on the grounds that the four institutions are private higher education institutions registered under the Private Higher Education Institutions Act 1996 and fall under the category of data user as specified in section 14 (1) of the Personal Data Protection Act 2010. In addition, the institutions have been in operation for more than 15 years and have their own privacy policy in force.

Being a qualitative study, this paper applies content analysis technique. This form of research involves categorizing the data collected into themes and sub-themes so that they may be compared (Moore & McCabe, 2005). On top of that, content analysis enables researchers to organise the qualitative data they have gathered in a way that fulfils the achievement of their research objectives. This is done by examining the data privacy policy of four private higher education institutions in Malaysia that are accessible on the official website of the institutions. As data users, private higher education institutions are required to communicate data privacy notices to data subject by one or more of the methods stipulated in paragraph 4.6 of the General Code of Practice of Personal Data Protection, and publication in the website of the data user is one of the methods.

7. Finding & Discussion

The analysis is structured based on the requirements of the General Code of Practice (CoP) of Personal Data Protection. Table 1 compares the privacy data practices in private higher education in Malaysia.

Table 1: Privacy Data Practices in Private Higher Education Institutions

No.	General CoP	UNITEN	UTP	TAYLOR'S	UNIVERSITY OF NOTTINGHAM
1	General Principle: consent by conduct/ performance and verbal consent.	By submitting personal data, the data user is deemed to have given his consent to the use of that personal data.	The notice does not expressly mention how consent is obtained but states that the university may collect information when the data subjects actively interact with the website and provide the information through the website. Withdrawal of consent can be done at any time by contacting the university in writing.	By using the website, data users are deemed to give consent to the collection/retention of personal information. For potential students applying for admission, they are required to provide a written consent using the form available on the admission section. The applicant and parent/guardian are required to sign the form to signify consent.	By agreeing to the terms of use, the data users are consenting to processing of personal data in accordance with the policy.

2	Notice and Choice Principle: Type of personal data collected and how, the use of personal data, the parties that the personal data is disclosed to and the choices including how to access and update the personal data.	Personal information to establish identity, contact information, payment information, sensitive information such as racial and ethnic origin, recording of image via CCTV, recording of photograph during event, recording of calls to customer service, function or post during commencement of business relationship, resumes when applying for job. Data collected either from data user, authorized representative, from third parties or from publicly available sources. Data will be used where permitted by applicable law and for the purposes stated.	Personal data provided voluntarily through website such as name, contact information, log-in information, browser type, operating system and URL information. The use of personal data only for the purposes specified in the policy.	Information collected: Personal details, respond to surveys and from usage of the website and any other information posted on website and email. Information collected and stored: name of domain from which date user access the Internet, the date and time of access and the internet address linked to the website. Use of information: Supply of goods, services and information, to ensure the content of the website is presented in the most effective manner, to analyze the information in order to improve and develop the website, provide information about product and services requested and to give notification about changes to the service. Information used to determine the number of visitors to different sections of the website.	Information automatically collected: IP address, dates and times of visit. Personal data: Name, address and email details. Withdrawal of permission to use personal data can be done by sending email to university.
3	Disclosure Principle: Disclosure is limited to the purpose and related purposes for which the original consent was given.	Third parties include federal and state government, law enforcement agencies, regulators, agents, contractors, service providers or professional consultants, business associates, other parties and	Access is limited to employees of the university and third-party agents. Personal data will be disclosed to third parties under a duty to disclose in compliance with legal obligation or to	Authorized personnel will have access to the information. The university may disclose the information to other third parties for the purposes set out. The university will not share, sell or	The data will not be disclosed to third parties other than in situations set out in the policy or with the permission from the data subject.

		credit reporting agencies.	protect the rights, property or safety of the university.	distribute information without consent unless required or permitted by law.	
4	Security Principle: Security standard for personal data processed electronically and non-electronically.	The university will take all reasonable steps to protect personal data that includes following security procedures but is not responsible for data policies, procedures or contents of other websites linked to the website of the university.	The university has reasonable security measures to help protect against the loss, misuse and alteration of the information under control.	Security measures are employed to protect information from unauthorized access and against unlawful processing, accidental loss, destruction or damage.	The website and the computer system have security measures to protect from loss, misuse or alteration.
5	Retention Principle: Retain data for as long as it is necessary to fulfil the purpose it was collected.	The university will retain personal data for the duration of the data subject's relationship with the university, for such a period as may be necessary to protect the interest of the university.	Personal data will be kept for as long as it is required to fulfil the purpose for which it was collected unless legal obligation requires it to be kept for longer.	The policy does not mention the retention period.	The university will retain the data for a reasonable period or for as long as the law requires.
6	Date Integrity Principle: Reasonable steps to ensure that personal data is accurate, complete, not misleading and kept up-to-date.	The university can assist data subject to access and correct personal data held.	The university aims to keep the information up-to-date and accurate as possible.	Nothing mentioned about this item on the policy or the notice.	The university will ensure that personal data is accurate, complete and up-to-date but it is not stated what steps or measures are in place.
7	Access Principle: Right to access and correct personal data.	In case the personal data is not inaccurate, incomplete, misleading or not up-to-date, the data subject may make a written request.	Data subject can review, change or delete the information by contacting the university.	Data users are encouraged to update the information by informing the university of any changes to email address and other contact details.	If there are any changes to personal data, the data users should notify the university via email.
8	Personal Data Protection Notice: Appendix 1	Not available online. The privacy policy provides for general provisions relating to personal data protection.	Available on the website. Five PDP Notice for different categories of data subject: For prospective	Available on the website. PDP Notice to students: Collect, use, store and destroy personal data for	Available on the website. The notice for the student, potential student, former student, client, customers,

			student, student and alumni, for visitor, for events, for job applicants and for employees.	various academic, educational and administrative purposes. Data collected: Name, identification number, passport number, address, contact numbers, gender, date of birth, qualification, email address, photo and images, marital status, emergency contact person and information about family/guardian. Sensitive personal data: Race, religion, records of misconduct and disciplinary action and criminal record.	potential customers, vendors, suppliers, service provider and/or relevant persons such as parent/guardian of student, potential student or former student, directors, employees of corporate customers, vendors, supplier, service provider and authorised representative receiving, obtaining services from and providing services to the university. Types of data and sources of personal data. Purposes of collecting data. Disclosure to parties listed in the Notice.
9	Personal Data Access Request Form: Appendix 2 Payment of fees, standard form for request, providing copy of the data within 21 days from the date of the receipt of Data Access Request.	Available on the website. The university shall inform the data subject in writing within 21 days for any data access made.	Form is not available. Any request to access may be made to the contact details (Legal Service Office).	Form is not available. Students have the right to access personal information in the student database system.	Form is not available. Requests for access or correction can be made in writing to the university with prescribed fee.
10	Personal Data Correction Form: Appendix 3.	Available on the website. The university shall inform the data subject in writing within 21 days for	Form is not available. Any request for modification or deletion may be made to the	Form is not available. Students are encouraged to notify the Campus Central of any	Form is not available. Data users should notify the university via email.

		any data access made. Requests can also be made to the Compliance Officer.	contact details (Legal Service Office).	changes in a timely manner.	
11	Notice under section 43 (1) PDPA to Prevent Processing of Personal Data for Purpose of Direct Marketing: Appendix 4	Not available on the website.	Not available.	Not available on the website.	Not available on the website.
12	Language Paragraph 4.5	Both versions in Bahasa Malaysia and English are available on the website.	Both versions in Bahasa Malaysia and English are available on the website.	Only the English version is available online.	Both versions in Bahasa Malaysia and English are available on the website.

The analysis on the privacy policy of UNITEN, Taylors' University, UTP and University of Nottingham found that the institutions have, to certain extent, complied with the requirements. They have the privacy policy published on the official websites and is accessible to the public. Publication of privacy policy on the website is one of the methods of communication stipulated by the General CoP for Personal Data Protection.

In relation to consent, different expressions were used to show how consent is deemed to have been given by the data subject to the university. This is consistent with the requirement provided by the General Code of Practice for Personal Data Protection which requires that consent may be given by conduct/performance or by verbal consent. It is submitted that by submitting information to the university either through electronic medium or by submitting a hard copy form has the same effect as giving consent. The types of information collected, processed and used by the universities are clearly stated in the policy. Furthermore, use of information and its disclosure is expressly dealt with in the policy. Thus, the data subject should be aware of his/her right before submitting any information to the university.

With regard to retention principle, all universities except Taylor's University provide for the requirement of retention period in dealing with personal data. However, the provisions do not mention the exact period that the university will keep the information. Even the PDPA itself does not define the phrase 'for as long as necessary' thus causing ambiguity in the interpretation of the phrase.

Three universities in this study except UNITEN have their privacy notice published on the official website. UNITEN have their privacy policy but they do not have their privacy notice published on the website as required by the General Code of Practice. UTP has five different privacy notices for five categories of data subject namely prospective students, students and alumni, visitors, events, job applicants and the employees while Taylor's privacy notice is for students only. On the other hand, University of Nottingham's privacy notice deals with a wide range of data users that includes the student, potential student, former student, client, customers, potential customers, vendors, suppliers, service provider and/or relevant persons such as parent/guardian of student, potential student or former student, directors, employees of corporate customers, vendors, supplier, service provider and authorised representative receiving, obtaining services from and providing services to the university. The personal

data access request form and personal data correction form are available on the website of UNITEN only whereas the other three universities do not provide such forms for the data users thus any request for access and for correction of personal data must be made by writing to the relevant contact person/department in charge.

In addition, it is noted that the notice under section 43 (1) PDPA to prevent processing of personal data for the purpose of direct marketing is not found in any privacy policy of the four universities in this study. This is one part of the requirements that must be examined and taken into account when developing the privacy policy.

Finally, it is further observed that UNITEN, UTP and University of Nottingham provide two versions of the privacy notice in Bahasa Malaysia and English as required by the Act and the Code. The privacy notice of the three institutions further stipulates that in the event of inconsistency between the English and Bahasa Malaysia versions, the English version shall prevail.

8. Conclusion and Future Recommendation

The study indicates that in the absence of a personal data protection code of practice for the education sector as a guideline, the data privacy practices of the institutions vary from one to another. While some of the privacy notices have provisions which are general in nature which may lead to confusion to the data subjects, the data privacy notices show that the four institutions have, to certain extent, complied with the requirements of the PDPA in general.

Although the PDPA provides a retention principle which requires data users to retain data for no longer than is necessary, the usage of the word 'necessary' is not defined in the Act, leaving the definition unclear. It was found the institutions used similar expressions in the privacy policy thus leaving data users in the dark over what constitutes necessary. Reference should be made to the General CoP of Personal Data Protection, in particular Appendix 1 which states that the period is seven years or as long as the data subject is a customer of the data user.

Even though section 7(1) (b) of the PDPA required data users to inform data subjects before collecting personal data, privacy policies are often broadly worded, which result in allowing data users to process personal data in a comprehensive way. On the same note, no definition of real and informed consent is provided in the Act, thus giving opportunity to data users to draft inadequate privacy policy disclosures that are complex to the ordinary people.

To overcome the issue of notice and consent, the Act should require data users to state the specific purpose the data is being collected and processed for. Data users should not be allowed to merely stating that data analytics will be performed. This requirement is necessary to avoid situations where the data users may circumvent the disclosure requirement by introducing an umbrella purpose that allows the purpose of processing data to be whatever they wish for it to be.

The findings of this preliminary study on the data privacy practices of the institutions will be of great reference and taken into consideration in developing a comprehensive privacy policy for Universiti Islam Selangor. On the same note, future research should be undertaken to develop a code of practice of personal data protection for the private higher education institutions to provide clear guidelines for the institutions towards compliance of the PDPA.

Acknowledgement
This study is funded by the Skim Geran Penyelidikan Inovasi KUIS 2022 (Geran Penyelidikan Sekunder) (2022/P/GPIK/GPS-001).

References

Addae, J.H., Brown, M., Sun, X., Towey, D. & Radenkovic, M. (2017). Measuring attitude towards personal data for adaptive cybersecurity. *Information and Computer Security, Vol. 25 No. 5, pp. 560-579.*

Ataei, M., Degbelo, A., Kray, C. & Santos, V. (2018). Complying with Privacy Legislation: From Legal Text to Implementation of Privacy-Aware Location-Based Services. *ISPRS Int. J. Geo-Inf. 2018, 7, 442.*

Fernandes, J., Machado, C. & Amaral, L. (2022). Identifying critical success factors for the General Data Protection Regulation implementation in higher education institutions. Digital Policy, Regulation and Governance, Vol. 24 No. 4, pp. 355-379.

Katulić, A., Katulić, T. & Hebrang Grgić, I. (2022). Application of the principle of transparency in processing of European national libraries patrons' personal data. *Digital Library Perspectives, Vol. 38 No. 4, pp. 399-411.*

Leng, O. T. S., Vergara, R. G., & Khan, S. (2021). Digital Tracing and Malaysia's Personal Data Protection Act 2020 amid the COVIS-19 Pandemic. *Asian Journal of Law and Policy, Vol. 1 No. 1 (July 2021).*

Moore, D. S., & McCabe, G. P. (2005). *Introduction to the Practice of Statistics (5th ed.).* New York, NY: W.H. Freeman & Company.

Noor Sureani, N., Awish Qarni, A. S., Azman, A. H., Othman, M. B. & Zahari, H. S. The Adequacy of Data Protection Laws in Protecting Personal Data in Malaysia. *Malaysian Journal of Social Sciences and Humanities, Volume 6, Issue 10 page 488 – 495.*

Pelteret, M. & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organi- zations. *Informing Science: The International Journal of an Emerging Transdiscipline, 19, 277-301.*

Sudarwanto, A.S. & Kharisma, D.B.B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime, Vol. 29 No. 4, pp. 1443-1457.*

Westin, A.F. (2003). Social and political dimension of privacy. *J. Soc. Issues. 2003, 59, 431-459*

Statute, Standard and Guidelines

Personal Data Protection Act 2001
Personal Data Protection (Class of Data Users) Amendment 2013
Personal Data Protection (Class of Data Users) Order 2013
Personal Data Protection (Compounding of Offences) Regulations 2013
Personal Data Protection (Fees) Regulations 2013
Personal Data Protection (Registration of Data User) Regulations 2013
Personal Data Protection Regulations 2013
Personal Data Protection Standard 2013