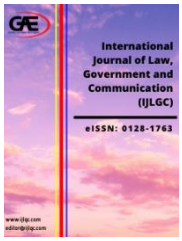
International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 9 Issue 35 (March 2024) PP. 45-55
DOI 10.35631/IJLGC.935005



INTERNATIONAL JOURNAL OF LAW, GOVERNMENT AND COMMUNICATION (IJLGC)
www.ijlgc.com

PERSONAL DATA PROTECTION POLICY: ENSURING EFFECTIVE IMPLEMENTATION OF DATA PRIVACY POLICIES IN PRIVATE HIGHER INSTITUTIONS

Suharne Ismail[1*]

[1] Faculty of Business and Management Sciences, Kolej Universiti Islam Perlis, Malaysia
Email: suharne@kuips.edu.my
[*] Corresponding Author

Article Info:

Article history:
Received date: 10.12.2023
Revised date: 18.01.2024
Accepted date: 15.02.2024
Published date: 01.03.2024

To cite this document:

Ismail, S. (2024). Personal Data Protection Policy: Ensuring Effective Implementation Of Data Privacy Policies In Private Higher Institutions. *International Journal Of Law, Government And Communication, 9* (35), 45-55.

DOI: 10.35631/IJLGC.935005

Abstract:

As digital technology develops globally, the protection of personal data in the commercial sector becomes extremely important. Cases of selling data to third parties are increasing, and the government is required to tighten provisions in personal protection laws. Therefore, the Personal Data Protection Act 2010 (Act 709) was passed by the Parliament of Malaysia for the purpose of regulating the processing of personal data and to prevent the misuse of the personal data in commercial transactions. The Act confers rights on Data Subjects in relation to the collection, use and or retention (processing) of their Personal Data, and places obligations on Data Users. The Personal Data Protection Order (Group Data Users) 2013 lists the categories of data users who need to register with Personal Data Protection Department. One of group data users is the education sector including educational institutions and private higher education registered under the Private Higher Education Institutions Act 1996 (Act 555). As data users, private higher education institutions are responsible for protecting Personal Data of two categories of data subjects, namely students and employees in the institution. The obligation including to exercise an appropriate policies and procedures to safeguard the Personal Data collected, to maintain data accuracy, and to prevent unauthorized disclosure. This paper aims to measure the implementation of personal data protection laws including the formulation of operational policies and procedures in private higher education institutions. This will be done by looking at the provisions from the Act regarding the principles of data protection as well as the duties for compliance to the legislation. Furthermore, non-compliance of the Act commits an offence and on conviction, be liable to a fine not exceeding RM500,000 or to imprisonment for a term not exceeding 3 years or both. The study also seeks to determine what are the challenges in implementing the Act successfully.

Keywords:

Data Protection, Personal Data, Privacy, Private Higher Education Institutions

International Journal of Law, Government and Communication
EISSN : 0128-1763
IJLGC
Volume 9 Issue 35 (March 2024) PP. 45-55
DOI 10.35631/IJLGC.935005

Introduction

Privacy is a fundamental human right that underpins freedom of association, thought and expression, as well as freedom from discrimination. Privacy includes the right to be free from interference and intrusion, to associate freely with whom you want to be able to control and also includes who can see or use our information. Even though there is no principle on the right of privacy in Malaysia, the Federal Court in the case of *Sivarasa v Badan Peguam Malaysia & Anor [2010] 3 CLJ 507*, ruled that the right to personal liberty under Article 5(1) of Federal Constitution includes the right to privacy. Privacy enables us to create barriers and manage boundaries to protect ourselves from unwarranted interference in our lives, which allows us to negotiate who we are and how we want to interact with the world around us. Privacy helps us establish boundaries to limit who has access to our bodies, places and things, as well as our communications and our information (Privacy International). Many organizations do not have a comprehensive, integrated, measurable, and centralized strategy for achieving data privacy compliance. To address customer concerns and to meet the legal requirements of personal data protection, many organizations disclose their information privacy practices through online privacy policy notices (Chua, Hui Na, et al,2017). According to Culnan, privacy issues can jeopardize the fiduciary relationship between an organization and its shareholders if the issues negatively influence stock price, causes the customer loss, and leads to legal fines (Culnan and Williams,2009). Meanwhile, (Earp, et al, 2009) examined that privacy policies are mostly written in a way that protects organizations from potential privacy lawsuits rather than addresses consumers' privacy concerns.

In 2019, the High Court delivered the decision in *Chan Ah Kien v Brite-Tech Berhad [2019] 1 LNS 2277*, in which a director of a listed company complained that his privacy was breached when his salary details were disclosed to third parties who were shareholders of the company. Azimah Omar J, dismissed the director's claim after having found that the director's salary in a listed company could not be considered private and confidential information, as those details are required to be provided in the company's annual report, which is a public document. In the case of *Ultra Dimension Sdn Bhd v Kook Wei Kuan [2004] 5 CLJ 285*, the appellant had taken a photograph of a group of kindergarten students in an open area outside the school and published it in two local newspapers as part of an advertisement campaign. The respondent, who was one of the students in the photograph, claimed that the appellant's actions amounted to an invasion of his privacy and a breach of confidence and he then sought damages from the appellant. The appellant however argued that there is no legal cause of action for invasion of privacy in Malaysia. Faiza Tamby Chik J agreed with the appellant. In *M Mohandas Gandhi v Ambank Berhad [2014] 1 LNS 1025*, the plaintiffs sued credit reporting agency, CITOS, for producing a report that included information relating to the plaintiffs' ongoing court case with a bank for alleged default on their loans. The plaintiffs argued that the information was private and that by publishing a public report, CITOS allegedly invaded their privacy. Lau Bee Lan J cited that the information was not private as it was already available in the public domain.

Literature Review

Privacy Law in Malaysia

The law of privacy in Malaysia is still grounded from common law and privacy protection from the judiciary is mainly on moral and chastity of women. Privacy rights are still mainly governed by Malaysia's Federal Constitution (Leng, O.T.S, Vergara, R.G., &Khan, S.,2021). Therefore, efforts should be directed towards introducing a robust and well-defined statutory tort of

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 9 Issue 35 (March 2024) PP. 45-55
DOI 10.35631/IJLGC.935005

invasion of privacy in Malaysia. This would provide a comprehensive framework for addressing privacy violations and better protect individuals' privacy rights in a legally enforceable manner (Adnan Trakic, Ridoan Karim, Hanifah Haydar Ali Tajuddin (2023).

In view thereof, the government of Malaysia introduce Personal Data Protection Act 2010 (Act 709) (hereinafter referred to 'the Act') and is a form of cyber legislation recommended the implementation of the Multimedia Super Corridor (MSC). Malaysia is the first among ASEAN members countries that enforce such an act. The main objective of this Act is set out in the Tenth Communications and Multimedia Act 1998, to ensure information security and network reliability and integrity. The Act is also to regulate the processing of personal data in commercial transactions and to provide for matters related and incidental thereto which mandates 13 industry sectors including Communications, Banking and Financial Institution, Insurance, Health, Tourism and Hospitalities, Transportation, Education, Direct Selling, Services, Real Estate, Utilities, pawnbrokers and Moneylenders to be registered under the Act. The Personal Data Protection Act 2010 is a step to overcome the problem of personal data intrusion which is getting worse in Malaysia. When this act comes into force, all aspects of personal data protection for commercial purposes will be guaranteed to be preserved (Trakic.A,2017). In the context of Malaysia, this Act is a data protection law that lays out requirements for commercial organizations to inform individuals about the purpose and extent of data collection, and to obtain explicit consent for such activities. However, the Act only applies to the private sector and not to the public sector since the government has its own database in each ministry.

The data privacy compliance applies to all the higher institution in safeguarding the information of the students and employees. The university is an organization that manages much public information, and therefore, information security policies are developed to ensure data security (Angraini, Alias, R.A., Okfalisa (2020). Data privacy compliance is a process that identifies the applicable governance for data protection, security, storage and other activities and establishes policies, procedures and protocols ensuring data is fully protected from unauthorized access and use. Therefore, failure to ensure compliance with information security laws poses significant financial and reputation risk and may invite serious scrutiny of university activities by law enforcement bodies (M. Kyobe,2010).

The importance of data compliance is to protect the information that the higher institutions use for their businesses/trades. Compliance with the data standards, regulations, and other governance rules and practices will ensure the confidentiality, integrity and availability of an organization's data. All the databases and other relevant information are securely managed and protected. To achieve a data compliance, higher institution must implement controls, policies and procedures and all related governance documents.

Methodology

The research methodology uses qualitative methods to observe and obtain the information on the implementation data policies in private higher institutions. This study is derived from certain journal, statutes, case law and articles that discuss the issues related to the implementation and enforcement of personal data policies and practices in private higher institutions. This means that secondary data and information are used to achieve the objectives of this paper. The analysis of this study is carried out by content analysis. Besides the case study approach, this study uses the literature review research approach on the studies by researchers who discussed the laws involved in the current Malaysian legal statutes.

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 9 Issue 35 (March 2024) PP. 45-55
DOI 10.35631/IJLGC.935005

Personal Data Protection Act, 2010

The Personal Data Protection Act, 2010 (PDPA) applies to any person who processes and any person who has control over or authorizes the processing of any personal data in respect of commercial transactions. Section 2 of the act defines ‘data user’ which is the equivalent of a 'data controller' as a person who either alone, jointly, or in common with other persons, processes any personal data or has control over, or authorizes the processing of any personal data, but does not include a data processor. Meanwhile ‘data processor’ shall process all personal data on behalf of the data user and/or provided by the data user (as the case may be) from time to time only for the performance of the data processor's obligations. For the purpose of this Act, the data processor shall be referred to as the Consumer and the data user is the Company. According to this Act, the data processor shall ensure that all the personal data that is in its possession is accurate, complete and up-to-date and to notify the data user in writing of any changes and updates on the personal data from time to time. The data processor shall provide full co-operation to the data user to ensure the full compliance with the Act.

According to the Act, ‘personal data’ relates directly or indirectly to a data subject, who is identified or identifiable from that information, or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject. Meanwhile ‘sensitive personal data’ means any data relating to physical, mental health or condition, political and religious belief as defined by law. *If sensitive personal data is collected, the purpose of the collecting will be explained to the data subject*. The Act does not permit the processing of sensitive personal data except for the purposes set out in the Act and such processing must be with the express consent of the data subject. The word of ‘processing’ under the Act means collecting, recording, holding or storing personal data or carrying out operation on the personal data including organizing, adapting, altering, retrieving, consulting, using, disclosing, making available, aligning, combining, correcting, erasing or destroying personal data. By virtue of this definition, the Act essentially includes any handling of personal data. However, the Act limits its application to only processing personal data in respect of ‘commercial transactions’, which carries the meaning of any transaction of a commercial nature, whether contractual or not, including any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance.

For the enforcement of this Act, the government of Malaysia has established Personal Data Protection Department (PDPD) is an agency under the Ministry of Communications and Multimedia Commission (MCMC). The main responsibility of this department is to oversee the processing of personal data of individuals involved in commercial transactions by data user that is not misused and misapplied by the parties concerned. The Act has mandated to all Personal Data User Group consists of individuals or private parties officially registered for the purpose of protecting the rights of consumers and the public. Data users should therefore ensure that there is full compliance with all the requirements under the Act and its subsidiary legislation, including the Personal Data Protection Regulation and the Personal Data Protection Standards.

Principles in Personal Data Protection in Malaysia

The Act asserts seven (7) Personal Data Protection Principles to be complied with when processing personal data which is stipulated in Division I of the Act. The first principle is the

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 9 Issue 35 (March 2024) PP. 45-55
DOI 10.35631/IJLGC.935005

general principle in Section 6. This principle prohibits the data user from processing a data subject's personal data without his/her consent unless such processing is necessary. In pursuant to Section 6(2)(b) of the Act, a data user may process personal data about a data subject if the processing is necessary:

a) for the performance of a contract to which the data subject is a party;
b) for the taking of steps at the request of the data subject with a view to entering into a contract;
c) for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract;
d) in order to protect the vital interests of the data subject;
e) for the administration of justice; or
f) for the exercise of any functions conferred on any person by or under any law.

The second data protection principle is notice and choice principle as stated in Section 7 where the data users must inform a data subject of a variety of matters which may relate to the latter's personal information which may need to be proceeded by or on behalf of the data user. The data user is bound to inform the data subject by written notice as to the type, purpose, extent, accuracy and consequences of the personal data being processed. Such written notice has to be given by the data user "as soon as practicable". The data subject can request in writing for the data user to cease processing their personal data. Failure to accord to such request without valid justification can be an offence.

While Section 8 is the third principle stipulated of disclosure principle. This principle prohibits the disclosure of personal data without the consent of the data subject except for some limited circumstances, such as for instances where the disclosure is authorized by the order of a court. The Act also imposes obligations on the data user to take reasonable steps or a specific measure to protect the data subject's personal data being processed from any loss, misuse, unauthorized or accidental access or disclosure, alteration or destruction. This is mentioned as the fourth principle in Section 9 of the Act.

The fifth principle in Section 10 of the Act is retention. This principle requires that personal data can only be retained for as long the main purpose for which it is must be processed has been fulfilled. The data user must destroy the data permanently once the data subject's personal data is no longer required for processing purposes. The sixth principle is data integrity principle as stated in Section 11 where the data user has an obligation to take reasonable steps to ensure that the data kept is accurate, complete, not misleading and up-to-date, having regard to the purpose of which the data was collected and processed. Meanwhile the access principle in Section 12 is seventh principle to be complied where the data subject has rights to access their own personal data and to correct the personal data which is inaccurate, incomplete, misleading or outdated, save and except under certain circumstances.

Application Personal Data Protection

Registration of Data Users

According to Section 14 of the Act, the data users who belongs to any class listed under the Personal Data Protection (Class of Data Users) Order 2013 are required to register as the data user. The requirement to register as a data user has been stipulated in Circular 1/2022 issued by the Department of Personal Data. To apply to be registered, a data user must provide

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 9 Issue 35 (March 2024) PP. 45-55
DOI 10.35631/IJLGC.935005

a copy of their constitution (previously known as memorandum of association and article of association), if the data user is a private or public company, or in other cases, a copy of constituent documents under which the data user is established. The application to be registered must be accompanied with registration fees depending on the type of establishment of the data user. A certificate of registration will then be issued to the data user if the application is successful, which would be valid for a period of not less than twelve months from the date on which the certificate of registration is issued. In section 16(4) sated that where a data user falls within the prescribed classes, processing personal data without a certificate of registration is an offence under the Act, which may attract liability to a fine up to MYR 500,000 and/or imprisonment up to three years. Failure of renewal may also result in a fine up to MYR 250,000 and/or imprisonment up to two years.

According to Section 17, the certificate of registration can be renewed and the application for renewal of the certificate of registration not later than ninety days before the date of expiry of the certificate of registration. It is also stated that when renewing a certificate of registration, the Commissioner may vary the conditions or restrictions imposed upon the issuance of the certificate of registration. The Commissioner also has rights to impose an additional conditions or restrictions and may refuse to renew a certificate of registration if the data user has failed to comply with any of the provisions of this Act. The commissioner also will refuse for issuance the certificate if it was induced by a false representation of fact by the data user or the data user has ceased to carry on the processing of personal data.

Data User Forum and Code of Practice

Personal Data Protection Act 2010 requires the Commissioner to establish the data user forum and code practice as mentioned in Section 21 and Section 23. These requirements enable the data user in a specified class to plan, develop and provide Code of Practice (COP) that would protect the rights of users in accordance with the provisions of the Act. The Code of Practice (COP) will become a guide to data users in order to ensure that the processing of personal data does not infringe a data subject's rights under the Act. From the data user forum, the Commissioner may review, modify and updating the COP from time to time. Any complaints or disputes from the data user forum would be suggest with an alternative procedure which is practical for determination of disputes. For this purpose, the Commissioner will register different COP for different classes of data users which consistent with the Act. The COP that has been registered will be make available to the public.

Section 25(2) stated that all data users belonging to a class of data users shall comply with the relevant registered code of practice that is applicable to that class of data users at a given time. Non-compliance of a data user with any provision of the code of practice that is applicable to the data user commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding one year or to both in pursuant of Section 29. As todate the following sector has registered COP with the Commissioner:

a. banking and financial – 19th January 2017
b. licensees under the Communications and Multimedia Act 1998 – 23rd November 2017
c. insurance and takaful industry – 23rd December 2016
d. transportation sector (aviation) – 21st November 2017

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 9 Issue 35 (March 2024) PP. 45-55
DOI 10.35631/IJLGC.935005

e. utilities sector (electricity) – 23rd June 2016
f. utilities sector (water); and
g. private hospitals in the private healthcare industry.

Rights of Data Subject

The Act has provided the rights of the data subject when the organization or a person processing their personal data which stipulated in Division IV of the Act. In Section 30 stated that the data subject has right of access to personal data. The data subject will be informed by the data user whether the personal data will be processed on by or behalf of the data user. The data user must be informed the purpose of the personal data processed and the reason for require the personal data. The data subject has rights to access on the personal data that it will not be disclosed to any third party without consent. The personal data will be kept and stored for the purposes it was collected from the data subject and cannot be used for other purposes. Right of access for data subject is to ensure that all the data obtained is accurate, up to date collecting the data is in accordance with legislation.

Meanwhile in Section 34 stated data subject has rights to correct personal data if the data is inaccurate, incomplete, mis leading or not up to date. The data subject may apply for the correction to the data user in writing to make a necessary correction or can withdraw their consent to the processing of the personal data. A data user who contravenes with this provision commits an offence and shall, on conviction, be liable to a fine not exceeding one hundred thousand ringgit or to imprisonment for a term not exceeding one year or to both. Section 42 of the Act mentioned on the rights of data subject to prevent the processing of personal data which is likely cause substantial damage or substantial distress to the data subject or to another person. The Act also provided a right to prevent processing of personal data for the direct marketing purposes. In pursuant of Section 43, a data subject may request the data user to cease or not to begin processing his personal data for purposes of direct marketing. Direct marketing is defined in Section 43(5) as the communication by whatever means of any advertising or marketing material which is directed to particular individuals. A data user who fails to comply with the requirement of the Commissioner commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.

Implementation Data Policy and Practices in Private Higher Education Institutions

Education sector is one of the classes listed under Personal Data Protection (Class of Data Users) Order 2013 including educational institutions and private higher education registered under the Private Higher Education Institutions Act 1996 and private school or private educational institution registered under Education Act 1996. In higher education, data privacy is particularly important to safeguard and protect employee information and student data. Failure to comply with privacy laws and regulations can result in substantial legal actions, sanctions, liabilities and penalties. The data subjects include students (prospective, actual and graduates), the institution's employees and also including any individuals involved in the data processing. Employee data are kept by employers, either for human resource management or to fulfil legal requirements of employment or social security legislation (Hassan,Kamal Halili). As the data subject, students have a right to confirm as to whether their personal information is being processed and then to receive a minimum set of information regarding the process of that processing. Here, the data user must describe the types of personal data collected, the

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 9 Issue 35 (March 2024) PP. 45-55
DOI 10.35631/IJLGC.935005

purpose of processing the data, the sources of the personal data, and the class of third parties to whom the personal data may be shared with.

Private higher institutions, as the data user must comply with all the Seven (7) principles in the Act. As for the first principle which is General Principle, the institutions are only allowed to process the personal data which has been given a consent by the data subject. The data subject in institutions involved students and the employees or any individuals involved in the data processing such as data of the spouse or guarantor in scholarship agreement. The personal data will be collected by the data user is relating to the personal information of the data subject such as name, address, national identity, or exam results. Other personal information of the employees and students are financial information, such as bank details and tax status, recruitment data, attendance and behavioural information, medical information, and staff development evaluations. Data subject must give consent by writing and duly signed to the data user to process the data. The private higher institutions must have a standard form or procedure to authorize them to process the personal data subject i.e., consent clause is incorporated in the data collection form. The management has an obligation to inform the data subject (employees or students) the purpose of the data will be processed and to whom they intend to disclose the data.

In order to comply with Notice and Choice principle in the Act, private higher institution must have a privacy notice that summarize the purpose for which personal data is being or is to be collected, used, disclosed and further processed. For the students, collection of personal data is for the application of admission, to assist in the placement of internship, for welfare, financial fundings or sponsorship. Also, it is for the purpose to provide ancillary services such as assistance with visa application and insurance coverage throughout your tenure of studies especially for the international students. The privacy notice should be made in national and English languages and also include the rights of data subject with that personal data. There are many departments and faculties or schools in private higher institutions sector which require different notice of privacy. The data user has an obligation to make a different or standard privacy notice that covers specific processing activities. The privacy notice must also include the procedure if the data is lost or stolen and the rules if the data will be transferred outside the institution. The privacy notice must have an element of client's friendly, understandable and excessive to the public and placed at the appropriate location and make available in the website.

Compliance with the Disclosure principle of the Act, the institution is not allowed to share only on limited circumstances and the disclosure is authorized by the order of a court. The personal data information of the employee will be kept by the Human Resources Department and as for the students will be handled by the Students Affairs Department. As for this purpose, the institutions will only disclose the personal information such as name, position, email address or the photos in the student's portal or the official website. Consent must be given by the employees or the students before any disclosure. Section 39 of the Act only permitted the disclosure for the purpose of preventing crime, investigations, court order and for public interest. The management in the institution shall provide comprehensive disclosure list in the collection data form. The disclosure list must contain the list of third party that the personal data may disclose i.e., The Ministry of Education, Foreign government departments if the students are enrolled in a foreign accredited programmed, Malaysian immigration department or foreign embassies. Where applicable, the disclosure list also includes third parties who

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 9 Issue 35 (March 2024) PP. 45-55
DOI 10.35631/IJLGC.935005

provide related services such as insurance agencies, Financial Aid Agencies, SOCSO, EPF, and external examination boards.

In the Security principle, the private higher institution must take a reasonable action to protect the personal data from any loss, damage, alteration or being misused by unauthorized party. Nowadays, with the growth of digitalization requires that all the personal information to be kept in softcopy. The manual filing system is still practiced today and requires strict control system to avoid any leakage of personal information. Several factors are taking into account for the institution to be considered such as the location of the personal data storage and the security measures which have been integrated within the equipment used to store the personal data. The institution must ensure to enhance the security system and the data security. Enhancing the data security by using Encrypt Data, keeping the devices secure and keep passwords private. Besides that, the institution must ensure that measures are taken to guarantee the integrity, reliability and competence of the staffs who have access to that personal data in order to secure on the transfer of all such data. Therefore, the cyber security practice plays an important role to ensure a good protection to personal data.

For the institution to comply with the fifth principle which is the Retention principle, there must be a standard procedure for the institution to retained the personal data or to permanently destroy. It is the duty of the data user i.e., the institution to effectively destroy or permanently delete such personal data once the purpose has been fulfilled. The institution has to determine the nature of the personal data as active, non-active, or archive. For the purpose of this principle, the data user needs to have a retention policy, a standard personal data review and disposal records or checklist. Personal data should be deleted at the end of the retention period. The retention period should be established and reviewed by the management such as retention period of five (5) years for the employee's files. They also must have a disposal record and the destruction method of disposal i.e., for paper by shredding and burning the sensitive document, For the digital or electronic the destruction method by deleting, reformatting or crushing the documents.

The Integrity principle is integrity where the institution must ensure the personal data accurate, up-to-date, truthful, and correct. According to Kristina Russo in Netsuite Portal, data integrity is the assurance that digital information is uncorrupted and dependable, so businesses can rely on the data to help inform key decision making. Data that lacks of integrity can mislead the users causing them of making unfortunate choices that can harm businesses and their stakeholders. The management in the institution shall requires their employees and students to update the personal data manually or electronics/online from time to time. The seventh principle in the Act is Access principle. Here, the employees and the students may have an access and correct their personal data by application to the management. The management of the institution shall provide a standard form for the purpose of this principle. To manage all the principles in accordance with the Act effectively, the institution should appoint Data Protection Officer to which has a responsibility to monitor internal compliance, inform and advise on data protection obligations and provide advice regarding data policies and practices.

Conclusion

With the growth of digital technology around the world nowadays, the protection of personal data in the commercial field is very important. The cases of selling data to third parties has been increased requiring the Government to tighten the regulation of the personal protection

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume 9 Issue 35 (March 2024) PP. 45-55
DOI 10.35631/IJLGC.935005

act. Although the private education sector is not risky compared to the financial and health sectors, a strict policy must be practiced in private higher institutions based on the Seven (7) principles in accordance with the act. Data protection policies and practices that has been established and used needs to be improved from time to time. Compliance to data protection policies will help the organization (private higher institution) to improve their corporate governance. Other than that, brand value as a private higher education will be improved by protecting data subject against unauthorized access. Additionally, with a good data protection policy will demonstrate the commitment in ensuring the protection and privacy of data subject.

Acknowledgement

The authors would like to acknowledge and extend special gratitude to Faculty of Business and Management Sciences, Kolej Universiti Islam Perlis (KUIPs) and Global Academic Excellence (M) Sdn Bhd., editor and reviewer for approving the publication of this article.

References

ABDUL GHANI, Fadhilah; AHMAD RAZALI, Nurulhuda; MOHD SHABRI, Syahirah. Akta Perlindungan Data Peribadi 2010: Satu Tinjaun. Jurnal Dunia Pengurusan, [S.l.], v. 3, n. 1, p. 1-8, mar. 2021. ISSN 2682-8251. Available at: <https://myjms.mohe.gov.my/index.php/jdpg/article/view/12529>. Date accessed: 28 oct. 2023.

Adnan Trakic, Ridoan Karim, Hanifah Haydar Ali Tajuddin, It is time to recognize the tort of invasion of privacy in Malaysia, *International Data Privacy Law*, 2023;, ipad016, https://doi.org/10.1093/idpl/ipad016

Angraini, Alias, R.A., & Okfalisa (2021). Affecting Factors in Information Security Policy Compliance: Combine Organisational Factors and User Habits.

Chan Ah Kien v Brite-Tech Berhad [2019] 1 LNS 2277

Chua, H. N., Herbland, A., Wong, S. F., & Chang, Y. (2017). Compliance to personal data protection principles: A study of how organizations frame privacy policy notices. *Telematics and Informatics*, *34*(4), 157-170.

Chua, Hui Na, et al. "Compliance to personal data protection principles: A study of how organizations frame privacy policy notices." *Telematics and Informatics* 34.4 (2017): 157-170.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. MIS quarterly, 673-687.

Data Privacy Laws: What You Need to Know in 2023 https://www.osano.com/articles/data-privacy-laws

Earp, J. B., Antón, A. I., Aiman-Smith, L., & Stufflebeam, W. H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management*, *52*(2), 227-237.

Farah Mohd Shahwahid & Surianom Miskam, (2014) Personal Data Protection Act 2010: Taking The First Steps Towards Compliance, E-proceedings, Conference on Management and Muamalah (CoMM 2014), (E-ISBN: 978-983-3048-92-2)

Kamal Halili Hassan,Personal data protection in employment: New legal challenges for Malaysia, Computer Law & Security Review,Volume 28, Issue 6,2012,Pages 696-703,ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2012.07.006.

Leng, O. T. S., Vergara, R. G., & Khan, S. (*2021*). Digital Tracing and Malaysia's Personal Data Protection Act 2010 amid the Covid-19 Pandemic

M Mohandas Gandhi v Ambank Berhad [2014] 1 LNS 1025

International Journal of Law, Government and Communication
EISSN : 0128-1763
IJLGC
Volume 9 Issue 35 (March 2024) PP. 45-55
DOI 10.35631/IJLGC.935005
M. Kyobe, "Towards a framework to guide compliance with IS security policies and regulations in a university," 2010 Information Security for South Africa, Johannesburg, South Africa, 2010, pp. 1-6, doi: 10.1109/ISSA.2010.5588651.

Official Portal Department of Personal Data Protection, https://www.pdp.gov.my

Personal Data Protection Act, 2010

Personal Data Protection Order (Group Data Users) 2013

Sivarasa v Badan Peguam Malaysia & Anor [2010] 3 CLJ 507

Sureani, N. B. N., Qurni, A. S. B. A., Azman, A. H. B., Othman, M. B. B., & Zahari, H. S. B. (2021). The Adequacy of Data Protection Laws in Protecting Personal Data in Malaysia. Malaysian Journal of Social Sciences and Humanities (MJSSH), 6(10), 488-495.

Rossana Ducato, Data protection, scientific research, and the role of information, Computer Law & Security Review, Volume 37, 2020, 105412, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2020.105412

Ultra Dimension Sdn Bhd v Kook Wei Kuan [2004] 5 CLJ 285

What is Privacy http://privacyinternational.org/explainer/56/what-privacy

Why are Ethics and Integrity is Essentials in Accounting. https://www.netsuite.com