Global Business and Management Research: An International Journal
Vol. 12, No. 4 (2020)

An Overview of the Personal Data Protection Act 2010 (PDPA): Problems and Solutions

Fadhilah Abdul Ghani *
Department of Business and Management, Universiti Tenaga Nasional Sultan Haji Ahmad Shah Campus
Email: AFadhilah@uniten.edu.my

Syahirah Mohd Shabri
Department of Business and Management, Universiti Tenaga Nasional Sultan Haji Ahmad Shah Campus

Maizatul Akmar Mohd Rasli
Department of Business and Management, Universiti Tenaga Nasional Sultan Haji Ahmad Shah Campus

Nurulhuda Ahmad Razali
Department of Business and Management, Universiti Tenaga Nasional Sultan Haji Ahmad Shah Campus

Emir Hambali Ahmad Shuffri
Department of Business and Management, Universiti Tenaga Nasional Sultan Haji Ahmad Shah Campus

** Corresponding Author*

Abstract
Purpose: To bring to the light a few weaknesses of the Personal Data Protection Act 2010 and provides suggestions as well as solutions.
Design/methodology/approach: This is a conceptual paper. The methodology of this research is by way of literature review. In this study, researchers' use secondary sources such as published research work, research articles, conference papers, dissertation and books.
Findings: The study argues that the Act (PDPA) is not comprehensive and need for amendments.
Research limitations/implications: This research only provides an overview of the Act (PDPA 2010)
Practical implications: Based on the result, the employers, especially the government, should realise that they need to develop some insights or solutions to the highlighted weaknesses.
Originality/value: -

Keywords: Data Protection, Personal Data Protection Act 2010, Breach of Data

Introduction

In anticipation of the 21st century, there have been a significant increase in the flow of information between organisations and consumers and thereby, it was encouraged that the exchange of information will possibly raise questions relating to the protection of data (Chua, H. N., et.al., 2017)**.** Data protection requires the applicable laws and regulations that make it illegal to store or exchange certain information about individuals without their knowledge or

consent (Cambridge Dictionary, 2020). Data protection regulations were designed to keep information safe and offer individual's protection whenever they are asked to disclose their personal data (Hockley, L., 2018).

Breach of data protection has become an important issue worldwide. The Kaspersky Lab, a Moscow-based cybersecurity company, reported that information regarding 30 million passengers' data for Malindo Air and Thai Lion Air were leaked online. Two former employees of the airlines' e-commerce contractors were responsible for the breach of the passengers' data and illegally accessed and kept the customers' personal data (Reuters, T. 2019).

The Personal Data Security Commission also reported that an upgrade to Grab's mobile application in August 2019 had exposed the personal data of more than 21,500 users to the possibility of unauthorised access (B., 2020). Besides, the global news source stated that it was suspected that a Chinese firm, Zhenhua Data, had collected personal data of 2.4 million people and that there were 1,400 Malaysians involved in a database leak involving 250,000 people (Barbaschow, A., 2020).

Malaysia has been graded in 2019, as the fifth-worst nation in terms of protecting the personal data of its people. The worst nation in terms of protecting the personal data of its people was China followed by Russia, India and Thailand (The Star, 2019). In 2019, 178 cases were reported compared to 64 cases in 2018. It was an increase of nearly 200 percent in data breach attacks (Rahimi Yunus, 2019). The number of cases in data breach attacks were increasing according to the Malaysian Computer Emergency Response Team of CyberSecurity Malaysia (Norazhar, D., 2019).

In realising the importance to mitigate the issue on the breach of data protection, the Personal Data Protection Act 2010 (PDPA) was enacted. However, despite the PDPA enforcement, cases of breach of data protection still existed. A few cases of breach of data protection have been reported and highlighted in the following sections.

Cases of Breach of Data Protection in Malaysia (2016 – 2020)

In 2016, personal details of possibly hundreds of thousands of secondary school leavers have been leaked to a private higher learning institution for marketing purposes (Mail, M., 2016). In the following year, in May 2017, a College operator Khas Cergas Sdn Bhd, which owns Victoria International College in Jalan Ipoh, was charged with processing the personal data of the college's former maintenance technician, A. Marimuthu, 39, without a certificate of registration issued by the Personal Data Protection Commissioner (M.Geswari, 2017).

In October 2017, more than 46 million mobile data subscribers in Malaysia has been leaked into the dark web through a massive data breach. The leaked details contain telephone numbers, single serial phone numbers and home addresses. Personal data were stolen from various public sector and commercial websites in Malaysia (BBC, 2017). In November 2017, CIMB Banking group had lost of several magnetic tapes containing back-up data. Some of those tapes contain customers' information of CIMB Bank and its subsidiaries (The Star Online, 2017).

Meanwhile in 2018, security breach involving details of organ pledgers happened. Total number of records leaked was 440,000, updated to 31 August 2016; it contains information from government hospitals and Malaysia's National Transplant Resource Centres (Babulal, V., 2018). Besides, Universiti Teknologi Mara (UiTM) also conduct an investigation-related complaint that more than 1 million personal students' data were leaked in a blog online (Babulal, V., & Jay, B. 2018).

Same goes to Universiti Malaysia Sabah (UMS), they did an investigation due to a hacker's group claim that they had stolen 50,0000 personal data and offered UMS students selling these data by uploading a status or posting on Twitter as well (Yeoh, A. 2019). While for University Malaya, an unidentified hacker had stolen nearly 24,000 user IDs, passwords, personal details

of UM's academic and non-academic staff from Universiti Malaya's (UM) online payment system e-pay (Yen Yap, M. 2019).
Recently, on 13 September 2020, The Malaysia Cyber Consumer Association (MCCA) makes the reports of unauthorized transfers of funds from the accounts, which have gone viral on social media. They also claim that they had been received numerous reports about that matter (NST, 2020).

Personal Data Protection Act 2010
The Personal Data Protection Act (PDPA) is the primary law regulating the protection of privacy in Malaysia. The Malaysian Parliament passed the law in May 2010 and on 2 June 2010, obtained the Royal Assent. By way of notification in the Government Gazette, the PDPA entered into force on 15 November 2013 with a three-month sunrise duration that ended on 15 February 2014 (Chia, J., 2014).
PDPA is an act regulating the collection of personal data in the context of commercial transactions. In other words, this act only covers privacy protection relating to commercial transactions, excluding its application over any other types of privacy interests (Chin, C., 2019).
During processing, the personal data must comply with these principles. Non-compliance by a data user with any of the standards constituted an offence under the PDPA and will be fine and/or imprisonment are included in the punishment. PDPA consisted of seven principles which are, general principle, notice and choice principle, disclosure principle, security principle, retention principle, data integrity principle, and also access principle (Kandiah, S., 2019). The detailed explanation of the seven data protection principles are as follows (PDPA, 2010):

General principle
The General principle prohibits the collection of personal data of an entity by a data user without their consent in compliance with legal requirements. The PDPA also forbids the processing of personal data unless it is directly related to the operation of the data subject to a specific reason; it is required for or directly related to that reason, and the data are processed in relation to that purpose is not excessive.

Disclosure principle
This principle forbids the disclosure, without the consent of the individual, of personal data for any reason other than the purpose for which the data was disclosed at the time of collection or for the purpose directly related to it; and to any party other than a third party of the class notified to the recipient of the data.

Security principle
The PDPA imposed responsibilities on the user of the data to take action to prevent personal data from any loss, misuse, modification, unauthorised or unintentional access or disclosure, alteration or destruction during its processing. The data user shall ensure that adequate assurances are issued by the data processor with regard to the technological and organisational security measures regulating the processing of the data and shall take appropriate steps to ensure compliance with those measures.

Data integrity principle
Users must act appropriately to ensure that personal data are correct, complete, and not deceptive and held up-to-date, taking into account the purpose for which they were obtained and processed.

Retention principle
The data user responsible shall take appropriate steps to ensure that all personal data are destroyed or removed completely if it is no longer needed for the purpose for which it was collected. Personal data must not be kept any longer than is appropriate for the reason for which it was collected to be fulfilled.

Notice and choice principle
Through written notice in both the national and English languages, the data owner is expected to inform the individual of certain matters, including the fact that the personal data of the individual was being processed and a summary of the data. The data user must give notice immediately when the data user first requested the personal data of the individual, or when the data user first gathered the personal data of the individual, or when the data user first utilised or disclosed it to a third party for a reason other than the original purpose.

Access principle
Provided the right of the person to view and correct his or her own information where it is incorrect, incomplete, misleading or obsolete. The PDPA offers grounds on which the data user may refuse to comply with the individual's request for data access or data correction.

Weaknesses of the PDPA 2010
Although the presence of the PDPA 2010 undeniably important, criticism still occurs, correlated with this statute and revealed that this act also appealed some weaknesses as well.

Only covers commercial entities
In other words, personal data collected in non-commercial transactions excluded and not protected by the PDPA. The term commercial transactions is defined under the PDPA to mean any transaction of a commercial nature, regardless of whether it is contractual. The PDPA will therefore affect how we use Personal Data in commercial, e-commerce and online transactions. Besides, there are no regulations directly covering the problems of online privacy including detail such as geolocation and cookies for instance. In 2017, a major data breach involving consumer data from an online message board was reported by over 46 million smartphone users in Malaysia (Fauzi N., 2019). This illustrates that there are still critical data management and security vulnerabilities, despite of the PDPA 2010.

No clauses available for parties to admit the breach of data
There is no clause available to make it possible for the parties to agree that their database has been compromised. An individual may submit their personal data in any survey or contest without consideration being given by any party (Yong Cieh, 2019).Legislation on personal data security should be allowed for businesses to provide the provision and give them a definitive plan of action on what needs to be done when a data breach happens, including advising their customers what they can do to mitigate the damage, such as changing passwords or asking their banks to update their credit card numbers (Says, 2017). In developing nations, regulation on personal data security allows companies to do so.

Government and State Government were exempted

The PDPA is not applicable to the Government and State Governments; it is only applied for the private parties. The draft of the PDP Bill specifically stated that the Government shall be bound by this Act. However, Section 3(1) of the PDPA for now reads, in a total reversal, this Act did not apply to the Federal and State Governments. The Government has not clarified the explanation behind this dramatic change. Furthermore, being one of the country's largest data consumers, the Government should be bound by the PDPA to avoid any sort of misuse of its citizen's personal data (Ahmed, S. M., & Zulhuda, S., 2019). However, there is still no legislation until today in Malaysia to control the collection and storage of personal information by Government bodies.

None independent PDP Commissioner

In definition, a Commissioner is a member of a commission or an individual who has been granted a commission. The PDP Commissioner is usually a person appointed by the Minister and to be accountable to the Minister, who may give him orders with accordance to the discharge of his duties and responsibilities (Cieh, E. L. Y., 2013). These regulations may obstruct the Commissioner's ability to perform his responsibilities and were not in line with international standards in requiring data protection. Moreover, a commissioner needs to be independent and to function free of political or governmental intervention.

Suggestions Solutions of the PDPA 2010

In 2017, a large data breach affected the online platform customers' data of more than 46 million mobile subscribers in Malaysia. The Minister of Communications and Multimedia, Mr. Gobind Singh Deo announced that by mid-2019, the Government was committed to a review of its data security legislation to deter data breaches from occurring (Fauzi N., 2019). Involving multi-type consumers with data from various industries required the compliance and application of Act 709, which needs to be further improved (Kandiah, S., 2019). This renewed commitment was essential in order to fill the weaknesses in data security and privacy.

Organisations and companies that gather, capture and store information must reconsider their security strategies by relying properly on employees the protection and privacy training. An employee who might not be trained in standard practices in security, had an inadequate password, visited fraudulent websites, clicked on links in unauthorised and suspicious emails, and blindly opened email attachments. This constituted a serious security threat to the systems and information of his organisation (Buang, S., 2017). Therefore, in order to ensure that employees recognize the importance of policy and practices to their positions, data users put in motion proper training and/or knowledge mechanisms for employees (PDP, 2017). This could be an initiative to evade some problems correlated to data breach from occurring in any company or industry.

Other recommendations to address the problem of this Act could be established by adding the right to enforce civil actions by a data user for redress and compensation in cases of breach of privacy. There is currently no other remedy for an aggrieved data subject for non-compliance with the PDPA 2010 other than to lodge a complaint with the Commissioner (Foong Cheng Leong, F., 2020). In the sense of common law, an aggrieved data subject could also seek civil action but depend on the circumstances of the situation. These proposed civil actions under the PDPA 2010 surely fill the void, particularly in issues relating to the abuse of personal data.

Conclusion

The above discussions briefly described an overview on the PDPA 2010 in Malaysia. Such legislation specifically sets out how data users can implement data privacy laws in order to guarantee and secure private and personal information by using the principles from this legislation. However, violation of data protection still occurred in this country and revealed all the shortcomings of this legislation as well. Therefore, the highlighted weaknesses should be improved.

References

Ahmed, S. M., & Zulhuda, S. (2019). Data Protection Challenges In The Internet Of Things Era: An Assessment Of Protection Offered By Pdpa 2010. *International Journal of Law, Government and Communication, 4*(17), 01-12. doi:10.35631/ijlgc.417001

B. (2020, September 12). *Singapore says Grab's fourth privacy breach is cause for concern*. Free Malaysia Today. https://www.freemalaysiatoday.com/category/business/2020/09/12/singapore-says-grabs-fourth-privacy-breach-is-concerning/

B. (2020b, September 15). *Putrajaya to check report about personal data leaked to China*. Free Malaysia Today. https://www.freemalaysiatoday.com/category/nation/2020/09/15/putrajaya-to-check-report-about-personal-data-leaked-to-china/

Babulal, V. (2018, January 25). *Security breach involving details of organ pledgers worrisome: Cybersecurity analyst.* Retrieved September 13, 2020, from https://www.nst.com.my/amp/news/crime-courts/2018/01/328687/security-breach-involving-details-organ-pledgers-worrisome

Babulal, V., & Jay, B. (2019, January 25). *UiTM to probe claims of data breach: New Straits Times.* Retrieved September 13, 2020, from https://www.nst.com.my/news/nation/2019/01/454429/uitm-probe-claims-data-breach

Barbaschow, A. (2020, September 24). *Australians are caring more about data privacy but don't know how to protect themselves*. ZDNet. https://www.zdnet.com/article/australians-are-caring-more-about-data-privacy-but-dont-know-how-to-protect-themselves/

BBC, N. (2017, October 31). *Malaysian data breach sees 46 million phone numbers leaked.* Retrieved September 13, 2020, from https://www.bbc.com/news/amp/technology-41816953

Buang, S. (2017, November 23). *Is data breach preventable?* NST Online. Retrieved September 30, 2020, from https://www.nst.com.my/opinion/columnists/2017/11/306329/data-breach-preventable

Cieh, E. L. Y. (2013). *Limitations of the Personal Data Protection Act 2010 and Personal Data.* Springer Link. https://link.springer.com/chapter/10.1007/978-3-642-33081-0_4

Chia, J. (2014, May). *Data protection in Malaysia - Taylor Wessing's Global Data Hub*. Global Data Hub. https://globaldatahub.taylorwessing.com/article/data-protection-in-malaysia

Chin, C. (2019, October 18). *Universiti Malaya: No data compromised in E-Pay portal hack*. The Star Online. https://www.thestar.com.my/tech/tech-news/2019/10/18/universiti-malaya-no-data-compromised-in-e-pay-portal-hack

Chua, H. N., Herbland, A., Sew, F. W., & Chang, Y. (2017, July 1). *Compliance to personal data protection principles: A study of how organizations frame privacy policy notices*. ScienceDirect. https://www.sciencedirect.com/science/article/abs/pii/S0736585316304336

DATA PROTECTION: Meaning in the Cambridge English Dictionary. (2020). Retrieved October 08, 2020, from https://dictionary.cambridge.org/dictionary/english/data-protection

Fauzi, N. (2019, February 12). *Data Privacy Law: Malaysia has a long way to go.* NST Online. https://www.nst.com.my/opinion/columnists/2019/02/459321/data-privacy-laws-malaysia-has-long-way-go

Foong Cheng Leong, F. (2020, February 25). *Public Consultation Paper No 01/2020 – Review of Personal Data Protection Act 2010 (Act 709) [14 – 28 February 2020].* Retrieve October 05, 2020, from https://foongchengleong.com/2020/02/public-consultation-paper-no-01-2020-review-of-personal-data-protection-act-2010-act-709-14-28-february-2020/

Hockley, L. (2018, August 15). *Why Is Data Protection Important? | DeltaNet*. DeltaNet International. https://www.delta-net.com/compliance/data-protection/faqs/why-is-data-protection-important

Kandiah, S. (2019, October). *Malaysia - The Privacy, Data Protection and Cybersecurity Law Review* - Edition 6 - TLR - The Law Reviews. Retrieved October 03, 2020, from https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210063/malaysia

Lim, I. (2020, October 2). *Ismail Sabri warns against naming Covid-19 patients, claims 'fake news' on positive cases in supermarkets, banks*. Malaysia | Malay Mail. https://www.malaymail.com/news/malaysia/2020/10/01/ismail-sabri-warns-against-naming-covid-19-patients-claims-fake-news-on-pos/1908510

M.Geswari. (2017, May 4). *College operator first to be hauled to court under PDP act*. Retrieve from The Star Online https://www.thestar.com.my/news/nation/2017/05/04/college-operator-first-to-be-hauled-to-court-under-pdp-act/

Mail, M. (2016, January 06). *Education Ministry confirms SPM, STPM student data leak: Malay Mail.* Retrieved September 13, 2020, from https://www.malaymail.com/news/malaysia/2016/01/06/education-ministry-confirms-spm-spm-student-data-leak/1035163

Norazhar, D. (2019, October 17). *Almost 200% increase in data breach attacks since...* The Malaysian Reserve. https://themalaysianreserve.com/2019/10/17/almost-200-increase-in-data-breach-attacks-since-2018/

Reuters, T. (2019, September 24). *Malindo data leak: Breach caused by ex-staff: New Straits Times.* Retrieved September 13, 2020, from https://www.nst.com.my/news/crime-courts/2019/09/524082/malindo-data-leak-breach-caused-ex-staff

Says, T. S. (2017, November 5). *Data breach opens up a can of worms.* Retrieved September 28, 2020, from https://www.thestar.com.my/opinion/columnists/the-star-says/2017/11/05/data-breach-opens-up-a-can-of-worms

The Star Online, H. (2017, November 13). *CIMB ups security after losing backup data.* Retrieved September 13, 2020, from https://www.thestar.com.my/business/business-news/2017/11/13/cimb-bank-steps-up-security-measures-across-all-channels/

Rahim, R. (2020, April 04). *MCCA probing spate of alleged unauthorised transactions at local bank: New Straits Times.* Retrieved September 13, 2020, from https://www.nst.com.my/news/crime-courts/2020/04/581274/mcca-probing-spate-alleged-unauthorised-transactions-local-bank

Yen Yap, M. (2019, October 21). *Nearly 45,000 University Malaya login IDs and passwords were leaked by an anonymous hacker*. Retrieved September 13, 2020, from

https://sea.mashable.com/article/6978/nearly-45000-university-malaya-login-ids-and-passwords-were-leaked-by-an-anonymous-hacker

Yeoh, A. (2019, November 05). *Hacker claims to have stolen personal data of Universiti Malaysia Sabah students.* Retrieved September 13, 2020, from https://www.thestar.com.my/tech/tech-news/2019/11/05/hacker-claims-to-have-stolen-personal-data-of-universiti-malaysia-sabah-students

Yong Cieh, E. L. (2019, September 16). *A Critique on the Personal Data Protection Act 2010 (PDP Act).* Retrieved September 28, 2020, from https://gltlaw.my/2018/08/01/a-critique-on-the-personal-data-protection-act-2010/