Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 488 - 495), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1087


**Malaysian Journal of Social Sciences and Humanities (MJSSH)**

Volume 6, Issue 10, October 2021

e-ISSN : 2504-8562

Journal home page:
www.msocialsciences.com

# The Adequacy of Data Protection Laws in Protecting Personal Data in Malaysia

**Nurkhairina Binti Noor Sureani[1], Atikah Shahira Binti Awis Qurni[1], Ayman Haziqah Binti Azman[1], Mohd Bahrin Bin Othman[1], Hariz Sufi bin Zahari[1]**
[1]Faculty of Law, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia

Correspondence: Mohd Bahrin Bin Othman (mohdb916@uitm.edu.my)

## Abstract

With the burgeoning technology, Malaysia has seen a staggering number of data breaches and data leaks within this past decade alone, with no signs of the trend decreasing. This has raised questions on whether the Personal Data Protection Act 2010 (PDPA) adequately protects the personal data of Malaysians. With the recent COVID-19 pandemic, data has been collected on a larger scale than before, with more frequent data leaks occurring. Hence, this study aims to analyse the adequacy of the PDPA by benchmarking it to the United Kingdom's (UK) Data Protection Act 2018, which have seen a decrease in data breaches since the implementation of the new legislation. In this context, personal data refers to information processed or recorded that relates directly or indirectly to a data subject, who may be identified from the information and may include sensitive personal data. The study uses a doctrinal analysis methodology to best explore the ideas and concepts within the literature available regarding the protection of personal data. The study also employs a comparative analysis methodology by comparing the scope and application of Malaysian and UK legislation for benchmarking. The findings suggest that there are improvements to be made for the PDPA to be adequate.

**Keywords:** personal data, data protection, data privacy, Personal Data Protection Act 2010

## Introduction

In Malaysia, the right to privacy is not expressly stated in the Federal Constitution. However, there are other entitlements enumerated specifically, the right to life and personal liberty, freedom of speech and assembly and freedom of movement (Ayub, 2018). Yaakob (2016) contends that although the right to privacy is not explicitly mentioned in the Federal Constitution, it is implied by Article 5(1) of the Federal Constitution whereby in *Sivarasa Rasiah v Badan Peguam & Anor (2010*), Justice Sri Ram (as he then was) stated in his obiter that personal liberty scope includes other rights, namely the right to privacy. The literature further proposes that the right to privacy is embedded in civil matters as evinced in *Lee Ewe Poh v Dr Lim Teik Man & Anor (2010)*, where the court held that the act of the plaintiff's surgeon taking pictures of the plaintiff's private parts amounted to a privacy breach (Halili, Abdelhameed and Ismail, 2018). Moreover, it was reinforced in *Lew Cher Phow @ Lew Cha Paw & Ors v Pua Yong Yang & Anor (2009)*, where the defendant's act in installing the CCTV directed at the plaintiff's front courtyard and the back of the plaintiff's house tantamounted to breaching the plaintiff's privacy, hence the court granted an injunction to prevent the defendant from installing CCTV targeted at the plaintiff's house.

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 488 - 495), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1087

However, Hashim and Mohd Yunus (2018) accentuate that the right to privacy in Malaysia is unclear, as elucidated in Sivarasah's case, the court did not further elaborate whether it wants to validate such a claim on breach of privacy. They further contend that the right to privacy is unclear because the term 'privacy' cannot be easily defined as it can be interpreted differently by individuals and the community. It is affirmed that Facebook's operation for privacy is not subject to any specific act or rules (Taib & Jamil, 2018). However, in the Malaysian Communications and Multimedia Commission, any actions that deviate from Malaysian jurisdiction can be enforced under the present law despite the method used.

The PDPA was passed by the Parliament in June 2010 and gazetted on 15 November 2013. It governs only matters involving data processing for commercial transactions, and there are seven principles laid down that data users must obey. The PDPA was proposed to elevate Malaysia as a hub for communications and multimedia focusing on e-transactions and investment, a test centre for digital communications technology, and a commerce partner in providing a global standard for personal data protection (Halsbury, 2017). The PDPA protects one aspect of privacy namely data privacy. Balasingam and Siddique Bhatti (2017) contend that the PDPA was enacted to support the right to privacy as the Human Rights Council conducted a Panel Discussion on the Right to Privacy in the Digital Age, which emphasises the need for privacy rights and examines ways to protect them in these days of technological advancement.

The PDPA aims to safeguard data subjects' personal data by controlling the person or organisation's act of processing, collecting, and keeping such data and standardising rules and regulations on the operation of personal data by any person or organisation. Data users must be registered under the PDPA and organisations must ensure compliance by taking certain actions regarding privacy matters (Abdul Rahim, Ismail & Samy, 2017). Lilynn (2017) purports that the object of the PDPA in regulating the process of personal data in commercial transactions have been further improved by the publication of the PDPA Standard 2015 and the Personal Data Protection (Class of Data Users) (Amendment) Order 2016. Yoon, et al (2019) stress the importance of the PDPA to safeguard data subjects' rights to privacy of the data processing as they have suffered various harms by the disclosure and misuse of their personal data.

## Literature Review

The background of this study analyses the application of the personal data protection law under the PDPA in Malaysia. Personal data is the information of an identifiable person in commercial transactions that may directly or indirectly relate to the data subject. Thus, the PDPA only safeguards personal data relating to commercial transactions (Basarudin et al., 2017).

The UK's Data Protection Act (DPA) 2018 took effect in May 2018 and replaced the DPA 1998 to keep the laws updated with the evolving digital age (Calder, 2016). Thus, a more comprehensive law on data protection was created, which may provide lessons for Malaysia in protecting personal data such as the areas covered by the DPA 2018 is broader specifically, to general data, law enforcement, the government sector, and other personal data, including non-commercial transactions (Swinhoe, 2019).

However, the literature states that the PDPA has notable shortcomings and loopholes, raising problems in safeguarding personal data (Islam & Karim, 2019). As of October 2019, the data shows a 200% increase in data breaches compared to only 63 cases in 2018, which shows an increasing need for better data protection laws to prevent data from being violated (Yunus, 2019). This indicates that as technology advances, there are a greater number of breaches. To address this issue, data protection law must be adequate to prevent data from being violated. Thus, there is a need to examine whether the PDPA is adequate and make recommendations to improve its application.

San explains that personal data is any information regarding commercial transactions in which the information is related to any person identified from the data, either directly or indirectly (San, 2020).

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 488 - 495), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1087

An individual may be identified by name, telephone number, date of birth, identity card number, and others (Information Commissioner Office, 2021). This information will be regarded as personal data if a person can be identified through it. Data protection law is created to protect matters relating to personal data and control the processing of the said data (Aggarwal, 2020). There are seven principles of data protection in Malaysia to ensure individuals' personal data is protected based on the EU General Data Protection Regulations (GDPR).

The literature shows that the lack of sufficient data protection laws leads to breaches in data, as evinced in Singapore whereby over 95% of the businesses were reported to be suffering from data breaches between September 2018 and September 2019 (Lago, 2020). With the implementation of the GDPR in European countries such as the UK, France, and Germany, there is less risk of data breaches. Only 79,000 companies compliant with GDPR suffered data breaches, which contrasts with 212,000 companies non-compliant with GDPR suffering from data breaches (Swinhoe, 2019). Thus, it shows an almost 63% reduction in the risk of a data breach if companies follow GDPR. Notably, Malaysia was ranked the fifth-worst country in 2019 regarding personal data protection, leading to a data breach (Abdul Ghani et al, 2020). For instance, a hacker stole the personal information of 24,000 passwords, user ID and emails from the University of Malaya's system (Yap, 2019).

The recent COVID-19 pandemic has raised concerns over data management such as geolocation, health information, and contact information that were given to help curb the pandemic (Kedzior, 2021). Zwitter and Gstrein (2020) raise concerns that collecting such data may be misused and will inevitably result in data breaches. If incorrectly handled such data collection will cause social and economic consequences, such as leak of personal information, targeted harassment, and interruption of economic flow.

Nevertheless, the literature shows a scarce comparison between Malaysia's PDPA and UK's DPA 2018, which denotes the gap in the data protection literature, as commentators prefer to benchmark the GDPR. This may be due to the DPA 2018 being recently amended or due to the UK recently finishing their transition period on 31 December 2020 after leaving the EU, which causes many parties to be uncertain on which data protection laws apply (Taylor, Wallace and Prictor, 2018). Thus, this study aims to shed light on using the DPA 2018 as a benchmark for the PDPA. Moreover, although the PDPA was enacted in 2010, there is still a gap in the literature regarding the adequacy of the PDPA in which this study aims to highlight.

## Methodology

This study adopts a qualitative methodology that comprises the doctrinal and comparative analysis of both the primary and secondary sources of law. The conceptual aspects of personal data protection are critically examined, which involves the concept and definition, characteristics, purpose, context, and the historical development of personal data protection. The final critical examination is on the literature concerning the relevant laws governing personal data protection in Malaysia and the UK. The primary sources in this study are the PDPA, Occupational Safety and Health Act 1994 (OSHA), Prevention and Control of Infectious Disease Act 1998 (PCIDA), the Measures (Within the Infected Local Areas) Regulations 2020, the GDPR, and the DPA 2018. This study applies the comparative research methodology by examining the data protection laws in the UK and Malaysia to recognise the gap in the PDPA. This is done by comparing these two systems, which subsequently draw a conclusion based on the findings from the DPA 2018 and PDPA.

## Result

### *The Right to be Forgotten*

The right to be forgotten or erased is essentially a fragment of personal data protection and the right to privacy (Haga, 2017). In the age of media and technology, information is kept as a memory that is

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 488 - 495), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1087

beyond the person's ability to memorise (Villaronga, Kieseberg & Li, 2018). Nevertheless, there are instances where erasing certain memories is important, especially in the digital world (Niessen et al., 2018). For example, a robbery suspect was released from prison five years later and decided to seek a job (Bouchagiar & Botis, 2018). Notably, Malaysia does not recognise the right to be forgotten compared to the UK (Azman et al., 2021). Though, commentators such as Walters, Trakman and Zeller (2021) contend that the notion of the right to be forgotten has been derived implicitly from section 10(2) of the PDPA, where data may be permanently erased if it is no longer used. However, Wahyuningtyas (2019) argues that the rights are only protected to a certain extent. It is further claimed that the provision is vague in which lawful grounds for a person to exercise the right to delete their personal information are not provided. According to Mohamed (2016), the right to be forgotten in Malaysia is an unformed clay that may lead to abuse if no specific and appropriate guidelines are given.

## *Compensation and Remedies*

Failure to conform with the seven key principles laid down under the PDPA would render the imposition of a fine on the data user, up to RM300,000 or up to two years of imprisonment, or both. In comparison to other jurisdictions, such as the UK, Malaysia does not impose revenue-based fines on a company's annual global revenue, reflecting the extent to which data security is offered in Malaysia. Furthermore, within the context of remedies, Mohamed and Zulhuda (2019) aver that an aggrieved person harmed by a breach of the PDPA's provisions could not initiate a civil action against the data used as the PDPA does not cover statutory civil right action. Instead, the civil claim must be pursued under common law or torts law for invasion of privacy due to data misuse or exploitation.

## *Commercial Transactions*

The scope of the PDPA in protecting personal data involving commercial transactions per se creates several drawbacks. The literature provides that it is difficult to differentiate between commercial business with the supply of goods and non-commercial business (Halili, Abdelhameed & Ismail, 2018). It is asserted that users' personal data in social media, which is most unsafe, is not preserved under the PDPA, thus, restricting the Act's application. Yusof, Ahmad and Mohamed (2016) have supported this, whereby the PDPA is inapplicable to data collection through social media especially, Facebook, Twitter and MySpace as it does not involve commercial transactions. This lack of protection has caused over 11 million Malaysian Facebook users' data to be leaked including their name, telephone number, birthday, the status of the relationship, and the date of account creation (Chapree, 2021).

Moreover, it is affirmed that the exemption of this Act for processing data by credit reporting agencies causes these agencies to disclose users' data without their consent or access to such data, hence defying the principles of the PDPA (Alibeigi & Munir, 2020). Kandiah (2020) further contends that the PDPA lacks certainty regarding the protection of social media user's personal data as it only covers commercial transactions. Basarudin et al. (2017) further explain that the data stored in the cloud for smart-home users too are not protected if their data is misused, leaving them with the option of only having a contractual agreement with the cloud service provider, which does not safeguard the processing of such data.

## *Exclusion of Governmental Bodies*

Notably, the PDPA excludes its application to the federal and state governments, which has an adverse effect as it gives the government unrestricted and absolute discretion whereby to safeguard the data subject's privacy, the same regulations must be applied to all data processors (Yaakob, 2016). Kwan (2020) avers that this exemption is obscure as the government holds all personal data of the citizen and foreigners. For instance, it is perceived that since the National Registration Department keeps all citizen data and income tax, misuse of personal data may occur because the data includes financial records and occupations; hence the government must be held accountable under the PDPA as this is valuable data that must be preserved. Song et al. (2010) support this view by arguing that although this

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 488 - 495), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1087

exemption is made for legitimate reasons, it makes the PDPA meaningless by excluding the body that stores and processes the most personal data in Malaysia.

It is also purported that this exemption would allow the Commissioner and the court to freely apply or interpret the Act, which raises critics among experts in data protection law as this exemption is only made by Malaysia and Singapore (Alibeigi & Munir, 2020). The issues on the PDPA has caused it to be reviewed under the Ministry of Communications and Multimedia.

### *Notice and Consent*

San (2020) observes that although section 7(1)(b) of the PDPA necessitates data users to inform data subjects to collect personal data, privacy policies are often broadly worded, allowing data users to process personal data in a very comprehensive method. Moreover, she claims that, despite consent being an imperative legal basis for processing, the Act does not define real and informed consent, allowing data users to draft inadequate privacy policy disclosures that are complex and intimidating to the layman.

### *Retention Period*

Although the PDPA provides a retention principle requiring 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 vague and gives room for data users to exploit the retention period (San, 2020).

## Discussion

### *Commercial Transactions*

As ostensibly discuss above, certain areas may not be governed by Malaysia's PDPA. This includes non-commercial transactions. The above analysis discovered that the word "commercial transaction" in the PDPA denotes the exclusion of activities beyond the commercial atmosphere which would unlock a doorway in creating privacy invasion of individuals, thus, causing data leaks. Therefore, it is recommended that the PDPA's scope be expanded to non-commercial transactions to establish a progressive society in Malaysia concerning personal data protection.

### *Exclusion of Governmental Bodies*

As mentioned earlier, the government is excluded from the PDPA's application. Thus, the PDPA may expand its scope by including governmental bodies to give adequate protection towards the personal data of the data subjects. The Act may direct how the government will use personal data. This will guarantee the government ensuring compliance with the seven principles of the PDPA when processing such data. The government may be held accountable in the occurrence of a breach in the processing of individuals' data, which would establish a more transparent act that creates safety and trust between data subjects and data users, subsequently giving protection to the personal data in Malaysia.

### *Notice and Consent*

To remedy the issue of notice and consent, the PDPA should require data users to state the specific purpose the data is processed for and must be prohibited from merely stating that data analytics will be performed. This is to avoid situations where the data user 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 PDPA should also include a guideline to standardise or detail a method of drafting a privacy policy notice that addresses the consumer's privacy concerns.

### *Emerging Technologies*

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 488 - 495), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1087

For the PDPA to sufficiently deal with emerging technologies, this research recommends that the PDPA's ambit should be widened to cover non-commercial transactions. This is because, in the Internet of Things era, many devices such as a smartwatch or smart homes collect and process important personal data such as geolocation, body and health measurements. However, as they are non-commercial transactions, protection cannot be offered to them in cases of breach or data leaks. Moreover, the blockchain participants must be identified as data controllers as they have the right to write on blockchain and decide to send data for validation by miners, have accountability in processing the data, and ensure compliance with their obligations under the PDPA. Therefore, this deals with the decentralised nature of blockchain by holding at least one party liable to the security and safety of the data collected and processed by blockchains.

Furthermore, to address the issue of the irreversible nature of blockchain, it is encouraged for the PDPA to include requirements for additional data contained in a transaction that includes personal data stored in a commitment scheme on a blockchain or is registered as a hash with encryption to establish confidentiality. Although this does not completely dismiss the challenges of the irreversible nature of blockchains in protecting personal data, it does provide a high level of security and confidentiality which regulates and provides a standard method of registration of personal data.

### *Transborder Data Flow*

This study has discovered that the absence of a list of certified countries for data transfer, the implementations and security measures on the process of data outside Malaysia in the PDPA weakens the criteria of Malaysia's adequacy to be seen and acknowledged as a safe country that secures personal data of its citizens. Hence, it is recommended to remove the whitelist from the Act and introduce new provisions on cross-border data flow by providing a clear guideline and safeguard measures in data processing especially on Malaysian data users across Malaysia to be recognised as a safe country.

## Conclusion

In conclusion, it is evident that the PDPA is a welcome step in data protection, but is still lacking, as compared to the UK's DPA 2018 in effectively protecting the personal data of individuals, as seen by the increasing cases of data breaches, data leaks, frauds, and scams in Malaysia. This study has surmised the lacunae seen in the PDPA on its scope, particularly on commercial transactions, exclusion of governmental bodies, notice and choice principle, emerging technologies, and the issue of transborder data flow. This study has offered recommendations to improve existing provisions in the PDPA as well as suggest new provisions to be included in the PDPA.

## References

Abdul Ghani, F. et al. (2020). An Overview of the Personal Data Protection Act 2010 (PDPA): Problems and Solutions. *Global Business and Management Research: An International Journal, 12*(4), 559-564.

Abdul Rahim, F., Ismail, Z., & Samy, G. N. (2017). *Healthcare Employee's Perception on Information Privacy Concerns.* (International Conference on Research and Innovation in Information Systems.

Aggarwal, S. (2020). *What is Data Protection and Why is it Important?* (Financial Express, 7 September 2020), <https://www.financialexpress.com/industry/technology/what-is-data-protection-and-why-is-it-important/2076419/> accessed on 30 January 2021.

Alibeigi, A & Munir, A. B. (2020). Malaysian Personal Data Protection Act, a Mysterious Application. University of Bologna Law Review, 52, 363-372.

Ayub, Z. A, & Mohamed Yusoff, Z.M. (2018). Right of Online Informational Privacy of Children in Malaysia: A Statutory Perspective. *UUM Journal of Legal Studies*, 221- 241.

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 488 - 495), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1087

Azman, A. et al. (2021). Privacy in the Era of Big Data: Unlocking the Blue Oceans of Data Paradigm in Malaysia. *Malaysian Journal of Social Sciences and Humanities*, *6*(5), 203-212.

Balasingam, U., & Siddique Bhatti, S. Q. (2017). Between Lex Lata and Lex Ferenda: An Evaluation of the Extent of the Right to Privacy in Malaysia. *Malayan Law Journal xxix*.

Basarudin, N. A. et al. (2017). Smart Home Users' Information in Cloud System: A Comparison Between Malaysian Personal Data Protection Act 2010 and EU General Data Protection Regulation. *Malaysian Construction Research Journal, 2*(2), 216.

Bouchagiar, G, & Bottis, M. C. (2018). *The Right to Be Forgotten: Memory Holes as the Default?* Amsterdam Privacy Conference.

Calder, A. (2016). *EU GDPR: A Pocket Guide*. IT Governance Publishing 2nd edn.

Chapree, C. (2021). *Personal Data of More Than 11 million Malaysian Facebook Users Leaked Online.* (Lowyat Net, 4 April 2021) <https://www.lowyat.net/2021/236599/personal-data-11million-malaysian-facebook-users-leaked/> accessed 13 June 2021.

Haga, Y. (2017). *Right to be Forgotten: A New Privacy Right in the Era of Internet.* New Technology, Big Data, and the Law 97-126.

Halili,K., Abdelhameed, A., & Ismail, N. (2018). Modern Means of Collecting Evidence in Criminal Investigations: Implications on The Privacy of Accused Persons in Malaysia. *International Journal of Asian Social Science*, 332-345.

Halsbury, H. S. G. (2017). Halsbury's Laws of Malaysia. *Malayan Law Journal, 16*.

Hashim, N. & Mohd Yunos, A. S. (2018). *Right to Privacy and Malaysian Practice: A Step Further in Recognising Another Aspect Human Rights.* 5th International Conference on Science and Social Research.

Information Commissioner's Office. (2021). *Guide to the General Data Protection Regulation (GDPR): What is Personal Data?* <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/> accessed 10 January 2021.

Islam, M.T., & Karim, M. T. (2019). A Brief Historical Account of Global Data Privacy Regulations and the Lessons for Malaysia. *Journal of History Department, University of Malaya, 28*(2), 169-186.

Kandiah, S. (2020). *The Privacy, Data Protection and Cybersecurity Law Review: Malaysia"* in Alan Charles Raul (ed) The Privacy, Data Protection and Cybersecurity Law Review (Law Business Research Ltd 2020) at p 283.

Kedzior, M. (2021). The Right to Data Protection and the COVID-19 Pandemic: the European Approach. *ERA Forum*, 533–543.

Kwan, C. K. H. (2020). *Data Privacy for Lawyers: An Introduction.* Legal Network Series (A) cxxxi.

Lago, C. (2020). *The Biggest Data Breaches in Southeast Asia.* CSO Online, 18 January 2020 <https://www.csoonline.com/article/3532816/the-biggest-data-breaches-in-southeast-asia.html> accessed 10 January 2021

Lee Ewe Poh v Dr Lim Teik Man & Anor [2010] 1 LNS 1162

Lew Cher Phow @ Lew Cha Paw & Ors v Pua Yong Yang & Anor [2009] 1 LNS 1256

Lilynn, S. (2017). *Brief Comparison Between the Malaysian Personal Data Protection Act 2010 and Other Jurisdictions.* Legal Network Series (A) xlvi.

Mohamed Yusof, N. A., Ahmad, N. A., & Mohamed, Z. (2016). A Study on Collection of Personal Data by Banking Industry in Malaysia. *Journal of Advanced Research in Business and Management Studies, 2*(1), 39-49.

Mohamed, D. (2016). The Privacy Right and Right to be Forgotten: the Malaysian Perspectives. *Indian Journal of Science and Technology, 9*(1), 1-7.

Mohd Taib, J., & Jamil, M. T. (2018). Internet Privacy Challenge for Facebook Users in Malaysia", Proceedings: Global Multidisciplinary Research Conference, Kuala Lumpur, 23 April 2018<http://www.mnnfpublisher.com/uploads/4/6/9/3/46931833/internet_privacy_challenge_for_facebook_users_in_malaysia.pdf> accessed 10 June 2021.

Niessen, C. et al. (2019). Time to Forget: Intentional Forgetting in the Digital World of Work. *Arbeit, 64*(1), 30.

Nurul Azma Saidi Abdullah, Md & Ab Rahman, Nurul & Chuah, Chai Wen & A Hamid, Rahmi, I. (2017). *Face Recognition For Criminal Identification: An Implementation of Principal Component Analysis For Face Recognition*, accessed on 4 June 2020, available

Malaysian Journal of Social Sciences and Humanities (MJSSH), Volume 6, Issue 10, (page 488 - 495), 2021
DOI: https://doi.org/10.47405/mjssh.v6i10.1087

athttps://www.researchgate.net/publication/320200512_Face_recognition_for_criminal_identification_An_implementation_of_principal_component_analysis_for_face_recognition.

San, T. P. (2020). The Impact of the Personal Data Protection Act 2010 on Data Analytics in the Retail Industry. *The Malayan Law Journal lxii-lxxxiii*.

Sidi Ahmed, S. M., & Sonny, Z. (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), 1-12.

Sivarasa Rasiah v Badan Peguam & Anor (2010) 2 MLJ 333

Song, C. W. et al. (2010). *Shielding Individual Peace in Modern Times: Debunking the Efficacy of the PDPA (2010) In Protecting Data and Privacy Rights"*, (University of Malaya Law Review, 19 April 2020) <https://www.umlawreview.com/lex-in-breve/shielding-individual-peace-inmodern- times-debunking-the-efficacy-of-the-pdpa-2010-in-protecting-data-and-privacyrights>accessed 29 January 2021.

Soon, V. R. H., & Cooray, M. (2021). Surveillance Technology and Cultural Notions of Privacy: Development of the Laws in Malaysia. *The Malayan Journal clxix.*

Swinhoe, D. (2019). *Does GDPR Compliance Reduce Breach Risk?.* (CSO Online, 20 March 2019) <https://www.csoonline.com/article/3369461/does-gdpr-compliance-reduce-breach-risk.html> accessed 10 January 2021.

Taylor, M. J, Wallace, S. E, & Prictor, M. (2018). United Kingdom: Transfers of Genomic Data to Third Countries. *Human Genetics, 137*(8), 637-645.

Villaronga, E. F., Kieseberg, P., & Li, T. (2018). Humans forget, machines remember: Artificial intelligence and the Right to Be Forgotten. *Computer Law & Security Review, 34*(2), 304-313.

Wahyuningtyas, Yuliana, S. (2019). *The Right to be Forgotten: Bargaining the Freedom of Information for the Right to Privacy?* in Khoo Ying Hooi and Deasy Simandjuntak (ed) Exploring the Nexus between Technologies and Human Rights: Opportunities and Challenges in Southeast Asia (Southeast Asia Programme (SHAPE-SEA) 2019) at pp 39-48.

Walters, R., Trakman, L., & Zeller, B. (2021). *Data Protection Law: A Comparative Analysis of Asia-Pacific and European Approaches.* e-book, <https://books.google.com.my/books?id=MmKtDwAAQBAJ&pg=PA212&lpg=PA212&dq=munir+on+the+right+to+be+forgotten+in+malaysia&source.

Yaakob, H. (2016). Facing Up to the Legal Challenges Arising from the Human Variome Project. *The Malayan Law Journal lxxix.*

Yap, M. Y. (2019. Nearly 45,000 University Malaya login IDs and passwords were leaked by an anonymous hacker. (Mashable SE Asia, 19 October 2019) <https://sea.mashable.com/article/6978/nearly-45000-university-malaya-login-ids-and-passwords-were-leaked-by-an-anonymous-hacker> accessed 30 January 2021.

Yoon, C. C. S. et al. (2019). An Evaluation of the Malaysian Personal Data Protection Act 2010 and the Singaporean Personal Data Protection Act 2012. *Legal Network Series (A) lxxxv*

Yunus, R. (2019). *Almost 200% Increase in Data Breach Attacks since 2018. The Malaysian Reserve (17 October 2019)* <https://themalaysianreserve.com/2019/10/17/almost-200-increase-in-data-breach-attacks-since-2018/> accessed 24 December 2020.

Zwitter, A., Gstrein, O. J. (2020). Big Data, Privacy and COVID-19 – Learning from Humanitarian Expertise in Data Protection. *Journal of International Humanitarian Action, 5*(4).