Malaysian Journal of Social Sciences and Humanities (MJSSH) (e-ISSN : 2504-8562)
2022, Volume 7, Issue 9, e001766
DOI: https://doi.org/10.47405/mjssh.v7i9.1766

The Australian Privacy Act 1988: Lesson to Be Learned

Mohd Bahrin Bin Othman[1*], Muhammad Faiz Bin Abu Samah[2]

[1]Faculty of Law, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia.
Email: mohdb916@uitm.edu.my
[2]Faculty of Law, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia.
Email: faiz.abusamah@gmail.com

CORRESPONDING AUTHOR (*):
Mohd Bahrin Bin Othman
(mohdb916@uitm.edu.my)

KEYWORDS:
Data Privacy
Data Protection
Privacy Act
PDPA
GDPR

CITATION:
Mohd Bahrin Othman & Muhammad Faiz Abu Samah (2022). The Australian Privacy Act 1988: Lesson to Be Learned. *Malaysian Journal of Social Sciences and Humanities (MJSSH), 7*(9), e001766. https://doi.org/10.47405/mjssh.v7i9.1766

ABSTRACT

Privacy is a fundamental human right recognized either explicitly or implicitly all around the world constitution. However, these privacy rights are being eroded by advanced technologies. The efficiency of the Australian Privacy Act 1988 being a non-European Union state in governing the protection of personal data is remarkable. The purpose of this paper is to shed light on how the Australian Privacy Act 1988 can be used as a benchmark for the Malaysian Personal Data Protection Act 2010. Thus, this paper employs a doctrinal qualitative method to best explore the ideas and concepts within the literature available regarding the legislation for the protection of personal data. It suggests that there are improvements to be made for the Malaysian Personal Data Protection Act 2010 to be adequate.

Contribution/Originality: The paper contributes to the existing literature on data privacy in Malaysia. Explicitly, it provides knowledge on how the Australian Privacy Act 1988, non-European Union legislation, was adopted and adapted with the GDPR. The Privacy Act 1988 can provide a good benchmark for the protection of data privacy in Malaysia.

1. Introduction

The lack of sufficient data protection laws leads to breaches in data whereby over 95% of the businesses were reported to be suffering from data breaches between September 2018 and September 2019 (The UK Government, 2021). With the implementation of the General Data Protection Regulation 2016 ('GDPR') in European Union ("EU") countries, 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 (Lago, 2020).

There is a need for the Malaysian Data Protection Act 2010 (PDPA) to be consistent with the GDPR. Thus, it is best for Malaysia to look into the Australian Privacy Act 1988 (Privacy Act) as a benchmark on how non-EU state legislation adapts to GDPR. The

Privacy Act is the principal piece of Australian legislation protecting the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information in the federal public sector and the private sector. The efficiency of the Australian Privacy Act 1988 being a non-EU state in governing the protection of personal data is remarkable.

2. Literature Review

The PDPA was established in 2010. PDPA aims to protect personal data that was collected for commercial transaction purposes (Section 2). The application and general principles of the Act have similarities with the Privacy Act practices in Australia. However, there are several differences and/or limitations of the PDPA compared to the legal provisions in Australia. In February 2020, the PDPC issued Public Consultation Paper No. 01/202 on the review of PDPA. However, there is no reported development about the PDPA Consultation Paper. Indeed, there is an urgent need to reform the PDPA to protect data efficiently (Othman al et., 2021). Several studies and research have pointed out the limitations of the PDPA from various aspects. The research in the study on the applicability of PDPA concludes that the Act's main limitation was regarding the issues of jurisdictional application. There is also a study that concerns the applications and principles of the PDPA (Jawahitha, Ishak & Mazahir, 2007).

The principal legislation protecting personal data in Australia is the Privacy Act. Morris (2020) briefly explained that this Act consists of 13 main rules that are meant to govern the management of personal data by both private and government sectors in Australia. In Australia, in the case of *Giller v Procopets [2008]*, individual personal data also receives additional protection from the common law associated with confidential information. The Privacy Act protects individual data that can either be information or opinions regarding a person. However, there are certain exemptions under the Privacy Act such as section 6D which excludes small and medium-size enterprise that generates an annual turnover of less than AUD 3 million. Although the intention of both the Privacy Act and PDPA is to protect personal information, the substance and effect of both Acts are very distinctive. Healey (2021) stated that the two Acts focus on the identification of data to actuate what is qualified as personal data.

3. Methodology

This paper applies a doctrinal methodology. It involved a comparative study between the Privacy Act, the GDPR and the PDPA. It analysed a set of secondary data obtained from the statutes, books, journals, online articles and viewpoints on the studies in personal data protection. It focused on the unit of analysis which consists of the principles of data protection, the remedies available to the data subject and the consequences for the breaches of the principles by the data user and data processor.

4. Result and Discussion

4.1. What Does the Privacy Act Provide?

The Privacy Act gives individuals the power to control their personal information. The Act listed the rights and principles to allow individuals to handle their personal information in determining the alteration of the data, access to personal information,

stop unwanted direct marketing use on their personal data, make a complaint for misuse of their data and the option to hide their identification.

4.2. Areas That the Privacy Act Are in Line with the General Data Protection Regulation

It is necessary to discuss the similarities and differences between Privacy Act and the GDPR. Both laws are similar in terms of rights and principles. For example, GDPR outlines requirements and six principles to be followed which is a similar concept to the 11 Information Privacy Principles ('IPP') under the Privacy Act and both include relation to the right to access and the right to be informed. Both define specific requirements for processing such data. In terms of definition, the Privacy Act refers to personal information which is in line with personal data under the GDPR.

4.2.1. The 11 Information Privacy Principles

According to Section 14 of the Act, every agency and federal offices that collect, utilize, and reveal any personal information must comply with the 11 IPP.

Principle 1 of the IPP stated the manner and purpose of the collection of personal information. The information must be necessary for the agency's work and collected fairly and lawfully (OAIC, 2018). The word fairly and lawfully can also be seen in principle 1 of the controller to adhere when processing personal data in GDPR. The latter talks about personal data being processed in a lawful manner, fairly and in a transparent manner.

Principles 2 of the IPP explained that an agency must tell individuals why they are collecting personal information, what laws give them authority to collect it, and to whom they usually disclose it (OAIC, 2018). This principle called solicitation of personal information from the individual concerned is in line with Article 13 of the GDPR which is the right to be informed. Article 13 summarizes that any gathering of data by companies, and individuals must be informed before data is gathered (OAIC, 2018). The said Article clearly states that "the controller shall provide the purposes of the processing for which the personal data are intended as well as the legal basis for the processing and the recipients or categories of recipients of the personal data if any;

Principles 3 of the IPP provided that an agency must take steps to guarantee that the individual data they collected is relevant, up-to-date, complete and not collected in an unreasonably intrusive way (solicitation of personal information generally). Likewise, in the GDPR, the data minimization principle and the accuracy principles state the data that is processed must be adequate, relevant, and limited to what is necessary for relation to the purposes for which they are processed. In addition, all personal data are processed to be accurate and kept up to date.

Both Principle 4 of the IPP and GDPR storage limitation principles mentioned storage. There is an addition to Principle 4 of the IPP about storage and security of personal information while GDPR storage limitation principles only talk about personal data are to be kept no longer than is necessary for the purposes for which the personal data are processed unless for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. However, in the GDPR, security was separated and listed as the final principle on its own which is called the security principle. The

same provides that personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage.

Principles 5-7 of the IPP requires agencies and offices to take precaution when holding a record of personal information and to allow people to access their personal information. Principle 7 of the IPP specifically the alteration of records containing personal information allows individual data to be corrected or rectified if the data is off-based. These principles are alike in the substance of GDPR rights to access which individuals have the right to request access to their data and to ask how their data is used by the company after it has been gathered. Similarly, principles of data can be corrected laid in the Act in line with the right to rectification in the GDPR under Article 16.

Principles 8-10 of the IPP discussed the rules on information use. Agencies must approximately keep precise, complete and up-to-date individual data, utilizing data for an important purpose, and only utilize the data for another reason in special circumstances, with the individual's permission or for the reason of health and safety or law enforcement reasons. If we're compared with the GDPR, this outline is similar to the right to restrict processing under Article 18. Though Article 18 provide the rights of the individual to request that their data is not used for processing and does not limit the processing under the individual's consent, the exercise of defence of legal claims or for the protection of the rights of another person or the public interest of the Union or of a Member State.

Lastly, Principle 11 of the IPP mentioned when an agency may reveal individual data to another agency. This comes under special circumstances related to an individual's authorization for health and safety or law requirement.

4.2.2. Definition of Individual

According to Article 3, 4(1) and Recitals 2, 14, 22-25, the GDPR only protects living individuals whose personal data of the deceased is not protected under GDPR. The Privacy Act protects the personal information of 'individuals,' defined as 'natural persons.' While not specifically noted, as an 'individual' implies a living person, the Privacy Act does not (except as specifically noted) apply to the information of or about deceased persons (Section 6 and Section 80G (2)). According to the Privacy Principles, the definition of personal information in Section 6 of the Act does not include deceased persons.

4.2.3. Territorial Scope

Article 3, 4, 11 and Recitals 2, 14, 22 to 25, the GDPR carefully explained that the GDPR applies to organisations set up within the EU notwithstanding whether the processing takes place within the EU or not. Similar to this, the Privacy Act also applies to APP entities and extends to all of Australia's external Territories (Sections 4 and 5A). Under the Privacy Act, any act done or practice in or outside Australia by an organisation or that has an Australian link is covered. What is an Australian link is if organisation consists of Australian citizens, continuous presence in Australia, a partnership formed in Australia, a trust created in Australia, or a body corporate incorporated in Australia

4.2.4. Special Categories and Sensitive Information

While the GDPR uses 'special categories of personal data to define personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometric data to uniquely identify a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, the Privacy Act chose 'sensitive information. Sensitive information refers to information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, a criminal record that is also personal information, health information, genetic information that is not otherwise health information about an individual, biometric information that is to be used for automated biometric verification or biometric identification and biometric templates.

4.3. Areas That the Privacy Act Are Not in Line with the General Data Protection Regulation

4.3.1. Personal Scope

The Privacy Act is subjected to Australian Government agencies and all businesses including nonprofit associations with a yearly turnover of more than $3 million. Small business organizations are also covered by the Privacy Act including private sector health service providers, businesses that sell or purchase personal information, credit reporting bodies, contracted service providers for Commonwealth contracts, employee associations registered or recognized, and businesses that choose to follow Privacy Act and are prescribed in the Privacy Regulation 2013. In addition, Privacy Act also covers a business that practices activities as part of their operations such as reporting entities or authorized agents relating to the Anti-Money Laundering and Counter-Terrorism Financing Act 2006, operation of a residential tenancy database, and activities related to the conduct of a protected action ballot.

The Privacy Act does not impose on state or territory government agencies including public hospitals and health care facilities, individuals acting in their capacity, public universities, public schools, small business operators, public media organisations and registered political parties and political representatives whereas under Regulation 56 (GDPR, 2016), in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

The GDPR applies to two kinds of company or business, one where the company or business established in the EU that processed personal information as part of their business or two, a company established outside of the EU and performs services to monitor the behaviour of citizens in the EU (European Commission, 2022). However, the GDPR does not apply to activities under the Law Enforcement Directive, or processing for national security purposes and personal processing or household activities (GDPR, 2016). The GDPR applies to two types of people, one is any individual regardless of their citizenship as long as they reside or are within the territorial boundaries of the EU and involves with the goods and services within the EU, and another is citizens of the EU regardless whether they presence within EU or not.

4.3.2. Entities

The GDPR defined data controllers and data processors which may be businesses, institutions, public bodies and nonprofit organizations86 while Privacy Act does not distinguish between both and applies to all entities. The Privacy Act uses the term agency or organization. According to Section 6 of the Privacy Act, an agency is defined to include Federal Public Authorities while the organization is defined to include an individual, a body corporate, a partnership, any unincorporated associated or a trust that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory. The GDPR provides protection that applies to all natural persons that reside in the EU (no matter what their nationality status) or to citizens of the EU (no matter where they are). The GDPR explicitly stated the word nationality in the definition, but the Privacy Act does not refer to nationality or place of residence in their Act.

4.3.3. Small Businesses

The differences can be seen with Privacy Act in terms of small businesses. There is no exemption available to small businesses in the GDPR. This is however contrast with the Privacy Act, whereby any small business operator is not an organisation and therefore is not an APP entity and not applicable to the requirements of the Act. As mentioned earlier, what is defined a as small business is a business whose annual turnover for the previous financial is less than $3 million (Section 6D of the Privacy Act 1988 and B.5 of the Privacy Principles Regulation). This means that small business is exempted from the APP requirement under Privacy Act.

4.3.4. Right to Erase

The GDPR provided rights to erasure without undue delay under circumstances (Article 12). When the consent of the data subject is withdrawn and there is no other legal basis for the data to be processed or data is no longer needed, the data subject has the right to request for their data to be erased from the record. The Privacy Act does not provide individuals with the right to erasure, unlike the GDPR. However, Principles 11.2 of the APP provides personal information must be destroyed or de-identified when the information is no longer needed or no longer requires to be retained.

4.4. What Can We Learn from the Privacy Act?

The Privacy Act is the principal piece of Australian legislation protecting the handling of personal information about individuals. This includes the collection, use, storage and disclosure of personal information in the federal public sector and the private sector (Raphael, 2019). The Privacy Act underwent major reform in 2014 and again in 2018 to enhance the protection of privacy in Australia. The Attorney General of Australia announced on December 12, 2019, that the Australian Government would conduct a review of the Privacy Act to ensure privacy settings empower consumers, protect their data, and best serve the Australian economy (Smith & Allens, 2019). As can be seen from the foregoing, the Privacy Act has always been reformed in order to keep up with current technology and extend its protections in accordance with the GDPR. Some of the provisions in the Privacy Act that the PDPA can consider adopting are its right to lodge a complaint with a supervisory authority as well as the external territories applicability of the Privacy Act.

Articles 79, 80, and 82 of the GDPR provide data subjects with the right to lodge a complaint with a supervisory authority. Article 33 of the GDPR also provides that a data user should notify of a personal data breach to the supervisory authority. It is similar to sections 25 and 52 of the Privacy Act which stated that individuals may submit a complaint about a breach of privacy to the Privacy Commissioner via the Office of the Australian Information Commissioner (Tay, 2020). This right should be adopted in PDPA to ensure the PDPA's efficiency in combating the issue of data breaches.

In addition, unlike the PDPA, which does not apply to personal data processed outside Malaysia, data protection under sections 4, 5A, 5B, and 6 of the Privacy Act applies to all agency or organisation entities and extends to all of Australia's external territories. The Privacy Act is also applicable to any act or practice carried out in or outside Australia by an organisation or small business operator with an Australian link. It is similar to the GDPR, which applies to organisations with a presence in the EU, particularly entities with an establishment in the EU, and applies to data processed by organisations with a presence in the EU, regardless of whether the processing takes place in the EU or not. The extraterritorial scope of applicability is critical, especially when it comes to protecting personal data involved in transborder data flows (Pardis, Johan & Ramanathan, 2018).

5. Conclusion

The discussion in this paper showcase that the Australian government has made a case for the application of existing laws to be adapted to the GDPR. Since Australia is another common law country, Privacy Act could be adapted to the GDPR effectively. In comparing the Privacy Act and the GDPR, the GDPR is a step forward. Australian businesses may need to comply if they have established their business in the EU or if they provided goods and services in the EU or to EU citizens. The study of the similarities and differences above shows that both privacy law includes some similar requirements. The GDPR and the Privacy Act require businesses to implement measures that comply with a set of principles and rights of individuals. Certain circumstances such as special categories under the GDPR are expected in similar circumstances of sensitive information in the Privacy Act.

Thus, it is beneficial for Malaysia to learn from the Australian on how to best adapt to the GDPR.

Acknowledgement

Part of this article was extracted from a Master of Enforcement Law project paper submitted to Universiti Teknologi MARA, Shah Alam, Selangor

Funding

This study received no funding.

Conflict of Interests

The authors reported no conflicts of interest for this work and declare that there is no potential conflict of interest with respect to the research, authorship, or publication of this article.

References

European Commission. (2022). Who Does the Data Protection Law Apply To?. *European Commission*. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en.

General Data Protection Regulation (GDPR). (2016). On the Protection of Natural Persons with Regard to the Processing of Personal Data and On the Free Movement of Such Data, and Repealing Directive 95/46/EC. *EUR-Lex*. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Giller v Procopets [2008] VSCA 236

Healey, R. (2021). Malaysia PDPA vs. GDPR: A Quick Breakdown. *Formiti*. https://formiti.com/malaysia-pdpa-vs-gdpr-a-quick-breakdown.

Jawahitha, S., Ishak, M. & Mazahir, M. (2007). E-Data Privacy and the Personal Data Protection Bill of Malaysia. *Journal of Applied Sciences*, 7,732-742

Lago, C. (2020 January). The Biggest Data Breaches in Southeast Asia. *CSO Online*. https://www.csoonline.com/article/3532816/the-biggest-data-breaches-in-southeastasia.html

Morris, M. (2020). *The Privacy, Data Protection and Cybersecurity.* Law Review.

Office of the Australian Information Commissioner (OAIC). (2018 October). Privacy fact sheet 1: Information Privacy Principles under the Privacy Act 1988. Office of the *Australian Information Commissioner (OAIC)*. https://webarchive.nla.gov.au/awa/20181010022244/law/privacy-archive/privacyresources-archive/privacy-fact-sheet-1-informationprivacy-principles-under-the-privacy-act-1988

Othman, M. B., Francis, B., Mohd Tasrib, M. A., Mohd Nor., M. A., & Hesham, N. I. (2021). Re-Thinking the Data Protection Act 2010: Regulating the Facial Recognition Technology. *Current Law Journal*, 1.

Pardis, M. T., Johan, S. S., & Ramanathan, D. (2018). Cross Border Data Transfer: Complexity of Adequate Protection and its Exceptions. *Computer Law & Security Review,* 34, 582–594

Raphael, T., Lim, K. M., Horton, F., Bunaramrueang, P., & Tham, B. (2019). Cross-Border Comparison of Privacy Laws. *Lee Hishammuddin Allen & Gledhill*. https://www.lh-ag.com/wp-content /uploads/2019/12/6_PDPA-Country-Comparison_RTnLKM.pdf

Smith, G. & Allens, E. C. (2021). The Privacy, Data Protection and Cybersecurity Law Review: Australia. *The Law Reviews*. https://thelawreviews.co.uk/title/the-privacy-data-protection-and -cybersecurity-law-review/australia

Tay, P. S. (2020). The Impact of the Personal Data Protection Act 2010 on Data Analytics in the Retail Industry. *Malayan Law Journal*, 3.

The UK Government. (2021). Countries in the EU and EEA. *The UK Government Website*. https://www.gov.uk/eu-e