

## Malaysian Personal Data Protection Act, a Mysterious Application

ALI ALIBEIGI & ABU BAKAR MUNIR <sup>†</sup>

### ABSTRACT

Malaysia is a pioneer in drafting and executing personal data protection law among the ASEAN countries. However, the adequacy of this protection regime is questionable. This study is aimed at evaluating the aptitude of the Personal Data Protection Act (2010) (P.D.P.A.) from the application perspective. The evaluation and analysis of the application and scope of the P.D.P.A. through comparative and descriptive approaches shows that the Act has provided for a narrow scope with wide exemptions. This approach may hinder a standard personal data protection legal system for the protection of individuals' privacy. Moreover, the P.D.P.A. will fail the adequacy test of the developed nations such as the European Union Member States.

### KEYWORDS

*Compliance; Information; Privacy; Personal Data Protection Act; General Data Protection Regulation*

### TABLE OF CONTENTS

Introduction . . . . .	363
1. Objectives of P.D.P.A. . . . .	363
2. Scope of P.D.P.A. . . . .	363
3. Application Exemptions . . . . .	365
4. Critique . . . . .	368
Remarks . . . . .	372

<sup>†</sup> Dr. Ali Alibeigi, Ph.D. in Cyber Law, University of Malaya (Malaysia); LL.M. in International Law (Osmania University, India); LL.B. (Hons) (Islamic Azad University, Iran). Dr. Alibeigi is a part-time lecturer, legal advisor and cyber law researcher. Contact: [alibeigi\\_a\\_80@yahoo.com](mailto:alibeigi_a_80@yahoo.com). Orcid id: 0000-0001-6927-6011.

Abu Bakar Munir, Professor of Law at University Of Malaya (Malaysia); member of the Academic Advisory Council of the Asia Pacific Institute for Digital Economy (Japan); member of the Asian Privacy Scholars Network (Australia). Professor Munir is an internationally renowned Visiting Professor, consultant and legal adviser on ICT Law, Data Protection Law, Nanotechnology Law, Renewable Energy Law and Policy. He is the author of several books and has widely published articles in reputable journals, including *Nature*. He was advisor to the government of Malaysia on crafting the 2010 Personal Data Protection Act and is currently assisting the government of the Republic of Indonesia in developing a personal data protection law. Contact: [abmunir@um.edu.my](mailto:abmunir@um.edu.my)

Acknowledgment - This research work has been funded by the University of Malaya Research Grant (UMRG), Project No: RP006C/13ICT. The authors would like to thank the University of Malaya for the financial support.



## INTRODUCTION

Malaysia, as a developing country, is impacted by new technologies. Hence, it is essential to understand if the present data protection laws and regulations are adequate to protect personal data of individuals. Legal analysis and benchmarking of the Personal Data Protection Act [hereinafter P.D.P.A.] will explore whether it can protect the personal data, solve the related legal disputes justly, and recover the damages completely.<sup>1</sup> However, the first and important step in the evaluation of a legislation is understanding its scope and application. An analysis of the objectives, scope and principles of the P.D.P.A. clarifies the need for a reform considering the change in circumstances and the fact that the Act was drafted many years ago.

### 1. OBJECTIVES OF P.D.P.A.

The P.D.P.A. commences with “*An Act to regulate the processing of personal data in commercial transactions and to provide for matters connected therewith and incidental thereto*”. The P.D.P.A. clarifies that it will protect the individuals’ personal information through governing the entire processing of such data from collection to deletion, with respect to commercial transactions only. Hence, the main objective of the P.D.P.A. is the protection of individuals’ personal data.

### 2. SCOPE OF P.D.P.A.

Under Section 2 of the P.D.P.A.,<sup>2</sup> it applies to the data users directly and to the personal data of individuals indirectly. Section 2(1) specifies that the P.D.P.A. applies to a person who processes the data or a person who has control over the information or authorizes

---

<sup>1</sup> The effectiveness of data protection laws will affect the consumers’ confidence and trust. For more information, see Gabriela Kennedy et al., *Data Protection in the Asia-Pacific Region*, 25 COMPUT. L. & SEC. REV. 59 (2009); Hamed Armesh et al., *The Effects of Security and Privacy Information on Trust & Trustworthiness and Loyalty in Online Marketing in Malaysia*, 2 INT’L J. MKTG STUD. 223, 223-234 (2010); Viviane Reding, *The Upcoming Data Protection Reform for the European Union*, 1 INT’L DATA PRIV. L. 3 (2011).

<sup>2</sup> Personal Data Protection Act § 2 (2012) provides that

(1) This Act applies to – (a) any person who processes; and (b) any person who has control over or authorizes the processing of, any personal data in respect of commercial transactions. (2) Subject to subsection (1), this Act applies to a person in respect of personal data if – (a) the person is established in Malaysia and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; or (b) the person is not established in Malaysia, but uses equipment in Malaysia for processing the personal data otherwise than for the purposes of transit through Malaysia . . . .

the processing. Personal information includes either manual data (filing system),<sup>3</sup> or electronic personal data, collected and used merely for the purpose(s) of commercial transactions by the private sector users. Personal information must be attached to the individuals, who are natural persons. The act applies solely to commercial transactions. Under Section 4 of the P.D.P.A., a commercial transaction means any commercial dealing of contractual or non-contractual nature,<sup>4</sup> with respect to supply or exchange of goods and services.<sup>5</sup> The relation between the employee and the employer under the employment contract also bears a commercial nature and falls under the governance of the P.D.P.A., although little attention has been paid to these types of data subjects. For the purpose of the Act, non-contractual transactions comprise informal or oral agreements. This definition is more or less similar to the interpretation of the Electronic Commerce Act (2006).<sup>6</sup>

Under section 2(2) of the P.D.P.A., subject to sub-section (1), the legislation applies to a “person” who is a data user and:

- a. is established within the territory of Malaysia and processes personal information “whether or not in the context of that establishment”;
- b. is established in Malaysia and process the personal data by employing a third party; and
- c. is not established in Malaysia, however, he bases his equipment in Malaysia to process the personal information.

Under Sub-section 2(3), this equipment must operate under an established representative in Malaysia to comply with the purposes of the P.D.P.A.. The important logical point under this provision is that the data user, especially a foreign data user, shall own the said equipment, so that he or she can be easily identifiable.<sup>7</sup> However, under Section 2(2) (b), a company which merely has equipment in Malaysia to transit personal data, is exempted from application of the Act. Although the term “transit” will fall under the ambit of “collection” of personal data, the P.D.P.A. has exempted these

<sup>3</sup> Filing system means paper based which is an old system of data recording.

<sup>4</sup> Most of the times, contractual transactions appear in the clearer form of written contracts.

<sup>5</sup> Personal Data Protection Act § 4 (2012) explains that

commercial transactions means any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance, but does not include a credit reporting business carried out by a credit reporting agency under the Credit Reporting Agencies Act (2010).

<sup>6</sup> Electronic Commerce Act § 5 (2006) on interpretation of the terms provided that: ““commercial transactions” means a single communication or multiple communications of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance.”

<sup>7</sup> ABU BAKAR MUNIR & SITI HAJAR MOHD YASIN, PERSONAL DATA PROTECTION IN MALAYSIA : LAW AND PRACTICE 78 (2010).

types of companies. This may be due to the encouragement to forge investments, especially of cloud companies. The P.D.P.A. exclusively applies to the private sector companies established in Malaysia or those that use equipment in the country. However, the term “equipment” has been criticized as being problematic.<sup>8</sup> Private sector includes all types of companies, such as Search Engine Marketing Companies.<sup>9</sup> In fact, the P.D.P.A. has provided for a “territorial jurisdiction”.<sup>10</sup>

Under the P.D.P.A., much concern has been given to the place of establishment, which is Malaysia. “Establishment” has been clarified in four circumstances by Section 2(4) to include:

- a. an individual who is physically being in Malaysia for more than one hundred and eighty days in one calendar year;
- b. a legal entity incorporated under Companies Act;<sup>11</sup>
- c. a partnership or any unincorporated association which is founded under any Malaysian legislation; and
- d. except the above mentioned categories, a person who maintains an office, branch or agency to conduct any activity within Malaysia or maintains a regular practice in Malaysia.

It would be more appropriate to use the phrase “data user” instead of “person” under Section 2. Hence, the P.D.P.A. regulates the whole processing operations of personal data for commercial transactions.

### 3. APPLICATION EXEMPTIONS

The exemptions are classified as total and partial exemptions.<sup>12</sup> Total exemptions mean that the P.D.P.A. will not apply totally, whereas, partial exemptions mean<sup>13</sup> only certain privacy principles will not apply to an activity. P.D.P.A. has provided certain total

<sup>8</sup> Abu Bakar Munir & Siti Hajar Mohd Yasin, *The Personal Data Protection Bill 2009*, 1 MALAY. L. J. CXIX-CXL, CXXVI (2010).

<sup>9</sup> Under the Australian Privacy Act (1988) and Japan Personal Information Protection Act (2003), small businesses are exempted. For more information, see Graham Greenleaf, *Malaysia: ASEAN's First Data Privacy Act in Force*, 126 PRIV. L. & BUS. INT'L REP. 12 (2013).

<sup>10</sup> Data protection laws usually apply three different approaches in order to determine their applications. Some of them rely on the location data user, some may rely on the location of the equipment used for processing and the rest consider the location of the individuals whom their data was processed. See Ustaran Eduardo, *The Scope of Application of E.U. Data Protection Law and Its Extraterritorial Reach*, in BEYOND DATA PROTECTION 135, 135-156 (Noriswadi Ismail & Edwin Lee Yong Cieh eds., 2013).

<sup>11</sup> Companies Act, 1965, (Publ. L. No. 125/1965).

<sup>12</sup> Munir Abu Bakar, *Personal data protection act : Doing well by doing good*, 1 MALAY. L. J. LXXXVII (2012).

<sup>13</sup> Personal Data Protection Act §45 (2012) has specified partial exemptions to the principles of the Act.

exemptions or non-application areas in order to limit the scope of the legislation (Table 1). There are two exemptions provided under Section 3 to specify delimitations of the P.D.P.A.:

- a. The Federal and state government; and
- b. Data processed wholly outside Malaysia.<sup>14</sup>

The Federal Government means the Government of Malaysia, including the Prime Minister's Office, Departments and all Ministries. The State Government is the government of a state which includes organizations such as the state secretary's office, state department, land and district offices and local authorities. However, the commercial companies owned by the Government are subject to the Act,<sup>15</sup> for instance, Khazanah Nasional Berhad<sup>16</sup> and Government Linked Companies.<sup>17</sup> Under Section 3(2), any personal data processed outside Malaysia is not subject to the Act, unless "intended" for further processing in Malaysia.

NO.	EXEMPTION	P.D.P.A. REFERENCE
1	Federal and State Government	Section 3(1)
2	Non-Commercial Activities	Section 2(1), Section 4 definition of "personal data"
3	Personal, Family or Household Affairs, Recreational Purposes	Section 45(1)
4	Credit Reporting Agencies	Section 4 definitions of "personal data" and "commercial transactions"
5	Information being processed outside Malaysia	Section 3(2)

Table 1: Non-application of P.D.P.A.

Under Section 4<sup>18</sup>, the personal data processed by credit reporting agencies are exempted from the application of the P.D.P.A., since credit reporting agencies are governed by a separate Act called Credit Reporting Agencies Act (2010) [hereinafter

<sup>14</sup> Personal Data Protection Act § 3 (2012) states that: "(1) This Act shall not apply to the Federal Government and State Governments. (2) This Act shall not apply to any personal data processed outside Malaysia unless that personal data is intended to be further processed in Malaysia".

<sup>15</sup> Greenleaf, *supra* note 9, at 11-12.

<sup>16</sup> Noriswadi has examined the status of the K.N.B. as an investment fund body of the government. He explains that K.N.B. assigned the responsibility of holding and managing the commercial assets of the Malaysian Government and to deal with strategic investments. Since the K.N.B.'s portfolio of companies is an incorporated body under the Companies Act 1965 and executes the "commercial transaction", hence the P.D.P.A. applies to it. Noriswadi Ismail, *Selected Issues Regarding the Malaysian Personal Data Protection Act (P.D.P.A.) 2010*, 2 INT'L DATA PRIV. L. 105, 109 (2012).

<sup>17</sup> Khazanah investment holding structure includes 54 companies. For more information, see: <http://www.khazanah.com.my/Home>.

<sup>18</sup> Personal Data Protection Act § 4 (2012) has excluded the credit reporting agencies under interpretation of the terms "personal data" and "commercial transactions".

C.R.A.A.].<sup>19</sup> Under Section 2(1) and Section 4 on definition of “personal data”, the P.D.P.A. only applies to the commercial transactions; hence, non-commercial activities of the private sector are totally exempted from the scope of P.D.P.A.. Non-commercial or non-profit activities by the private sector like charities, churches and non-profit organizations are excluded from the term “commercial transitions”. However, if a private company, which has been established for non-commercial activities, processes personal data for a commercial purpose, it will be subject to the P.D.P.A. for that operation even if the profit from that activity is used for non-commercial purposes.

Section 45(1) of the P.D.P.A.<sup>20</sup> has exempted personal, family and household affairs and recreational purposes from its application. For instance, a personal telephone notebook containing the names and phone numbers of friends, relatives or others will fall under this exemption. These affairs are not commercial in nature, and non-commercial activities are excluded from the ambit of the Act. This approach is similar to the Asia-Pacific Economic Cooperation Privacy Framework,<sup>21</sup> and Directive 95 that has excluded the processing of personal information by individuals “in the course of a purely personal or household activity”.<sup>22</sup> Furthermore, under Section 45, the P.D.P.A. has provided for partial exemptions for some kinds of activities in which some principles or provisions of the P.D.P.A. will not apply. For instance, processing of personal data for journalistic, literary or artistic activities is partially exempt from application of six principles of the Act.<sup>23</sup> It seems that the said exemption is in line with the freedom of expression and also freedom of press. According to Greenleaf, this exemption has been carefully drafted and is not a blanket media exemption.<sup>24</sup> Nevertheless, its application will be a complex issue.<sup>25</sup> The processing of personal data for prevention or detection of crime, investigation, apprehension or prosecution of offenders, taxation, physical or

<sup>19</sup> Credit Reporting Agencies Act, 710 (2010) entered into force on 15 October 2014.

<sup>20</sup> Personal Data Protection Act § 45(1) (2012) states that: “There shall be exempted from the provisions of this Act personal data processed by an individual only for the purposes of that individual’s personal, family or household affairs, including recreational purposes”.

<sup>21</sup> Asia-Pacific Economic Cooperation Privacy Framework § 10 (Nov. 2004) provides that: “[I]t also excludes an individual who collects, holds, processes or uses personal information in connection with the individual’s personal, family or household affairs”.

<sup>22</sup> Council Directive 95/46, art. 3(2), 1995 OJ (L 281).

<sup>23</sup> Personal Data Protection Act § 45(2) (f) (2012).

<sup>24</sup> See Graham Greenleaf, *Limitations of Malaysia’s Data Protection Bill*, 104 PRIV. L. & BUS. INT’L NEWSL. 5 (2010).

<sup>25</sup> Greenleaf, *supra* note 9, at 3.

mental health, statistics or carrying out research,<sup>26</sup> order or judgment of a court and discharging regulatory functions are partial exemptions provided under Section 45.

Although partial exemptions are broad to a certain extent, there is no blanket exemption from security principle, data integrity principle, and retention principle.<sup>27</sup> Furthermore, six exemptions are stated under Section 6(2) on General Principle.<sup>28</sup> Processing of personal data for performance of a contract to which the individual is a party, request of data subject to enter into a contract, legal obligation, protecting vital interests of data subject, administration of justice and performance of functions granted by individual or any law are exempted from the application of the general principle. However, the phrase “vital interests of the data subject” is vague and may cause legal conflicts. Moreover, under Section 46, the Minister is empowered to impose further exemptions, in addition to Section 45. The Minister, upon the recommendation of the commissioner, may exempt a data user or a class of data users from the application of any principles or any provision of the Act, and the Ministerial order must be published in the Gazette.

#### 4. CRITIQUE

A question arises as to whether a Data Protection Act, including these areas of exemption, can protect the personal information of the citizens properly? The P.D.P.A. has been criticized on the grounds that it has a narrow scope affected by wide limitations.<sup>29</sup> According to Graham, the P.D.P.A. applies to a part of private life, and has several exceptions.<sup>30</sup> He argues that the exemption of the government from application

<sup>26</sup> Oscar and Orville written a paper to address how can balance the right to privacy and the need for research to advance science to be headed by scientific community. They have discussed and examined seven principles to address the issue of growing imbalance between the need for research and privacy. See Oscar M. Ruebhausen & Orville G. Brim, *Privacy and Behavioral Research*, 65 COLUM. L. REV. 1184 (1965).

<sup>27</sup> See Greenleaf, *supra* note 24, at 5; Greenleaf, *supra* note 9, at 3.

<sup>28</sup> Personal Data Protection Act, § 6(2) (2012):

Notwithstanding paragraph (1)(a), 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.

<sup>29</sup> For more information, see Sidi Mohamed & Sonny Zulhuda, *Data Protection Challenges in the Internet of Things Era: An Assessment of Protection by P.D.P.A. 2010*, INT’L J. GOV’T COMM’N, Dec. 2019, at 1; Greenleaf, *supra* note 9; Greenleaf, *supra* note 23.

<sup>30</sup> Greenleaf, *supra* note 9, at 11.

of the P.D.P.A., together with the concept of commercial transaction, will grant freedom to the courts and the Commissioner to interpret the scope of the Act.<sup>31</sup> Moreover, excluding the Government from the application of the legislation is against the main purpose of the P.D.P.A..<sup>32</sup> This approach was severely criticized by data protection law professionals, as Malaysia and Singapore are the only countries who exempted the government from the data protection regime.<sup>33</sup> These criticisms have been enhanced by an ongoing legal debate about the definition and boundaries of the Federal Government, and the categorization of departments under the State Governments.<sup>34</sup>

The silence of the P.D.P.A. has only added to this controversy. However, the Interpretation Acts of 1948 and 1967 have defined the Federal Government and State Government. Under Interpretation Acts 1948 and 1967, the Federal Government means the Government of Malaysia, including all the Ministries and the Prime Minister's Department. The State Government means a government of a state, including some organizations like the State Secretary's office, State Department, land and district offices and local authorities. The Government Proceedings Act 1956 has the same definition of Government.

The presence of these definitions suggests that the wide criticism of the exemption of the Federal and State Governments from the application of the Act is perhaps a political issue with no legal concern.<sup>35</sup> However, the exemption remained a contentious issue since the moment of drafting of the Personal Data Protection Bill (2001). At the time, Mohamed Nor, the officer responsible for the data protection in the Ministry, had stated that the public sectors, with regard to the privacy issues, are adequately governed by the Official Secret Acts (1972) [hereinafter O.S.A.], Section 4 of the Statistics Act (1965), Section 19 of the National Land Code and Section 139 of the Consumer Protection Act (1999). Additionally, there are indirect protections of the data subjects by means of the disciplinary legislation and the administrative measures.<sup>36</sup>

---

<sup>31</sup> *Id.* at 12.

<sup>32</sup> Although most of governments collect a huge amount of individuals' data to develop their statistical bases through which, they will be able to plan and execute the governmental duties, however they have to observe and protect individuals' right over their personal data.

<sup>33</sup> Blume believes that a separate data protection law for the private and public sector at this situation would be a proper mechanism in order to empower the data subjects in protection of their personal data. See Peter Blume, *The Inherent Contradictions in Data Protection Law*, 2 INT'L DATA PRIV. L. 24, 24-33 (2012).

<sup>34</sup> Under the Interpretation Acts of 1948 and 1967, Federal Government means the Government of Malaysia including all ministries and Prime Minister's Department. The State Government means a government of a state including some organizations like the state secretary's office, state department, land and district offices and local authorities.

<sup>35</sup> Moreover, legally the nature and value of the personal information is the same whether uses by private or by the government.

<sup>36</sup> See Sarabdeen Jawahitha, Mohamed Ishak & Mohamed Mazahir, *E-Data Privacy and the Personal Data Protection Bill of Malaysia*, 7 J. APPLIED SCI. 732, 740 (2007).



The former Information, Communications, Culture and Arts Minister, Datuk Seri Dr Rais Yatim, also justifies the exemption of the government from the P.D.P.A. on the ground that the alternative rules and measures, such as O.S.A. and the laws pertaining to creditors, control the government.<sup>37</sup> Defenders believe that the Government exemption provides a right to process citizens' information for legal-administrative objectives. However, it was argued that O.S.A. applies to the government to protect official secrets like official documents, information and material for national security reasons, which has different scopes and objectives.<sup>38</sup>

The Singaporean model would be a good solution in order to minimize ambiguities and inconsistencies in the present model. The Ministry of Communications and Information of Singapore has developed the Personal Data Protection (Statutory Bodies) Notification 2013, which had entered into force on 20 March 2013.<sup>39</sup> It listed 67 public agencies which are exempted from the application of the Singapore Personal Data Protection Act 2012. In contrast, Section 45(2) (e) of the P.D.P.A. provided a broad exemption, which can be used as a measure to exempt government-owned companies from some of the provisions of the P.D.P.A..<sup>40</sup> Moreover, exclusion of the government could stem from the general exemption of non-commercial activities, which seems to be a defect of the P.D.P.A., and is not common under personal data protection laws.<sup>41</sup> This solution will result in confusion in practice. For example, a charity foundation engages in any commercial activity in order to provide scholarship funds for poor students. Sometimes, it is difficult to distinguish between commercial and non-commercial activities.<sup>42</sup> Moreover, social media are widely used by Malaysians. If we limit the P.D.P.A. to only commercial purposes, social media will be exempted, unless they are used for commercial activities.

The C.R.A.A. exemption under Section 4 on interpretation of the terms is not an appropriate position. It would be more appropriate to include this exemption under Section 3 which pertains to non-application of the Act. Furthermore, the business of Credit Tip Off Services Sdn. Bhd (CTOS), a big credit information agency and the primary source of credit referencing information before the C.R.A.A., has been criticised for opposing the P.D.P.A. principles. Moreover, it lacks the consent of the individuals for disclosure of their personal information, and they do not have access to their data.<sup>43</sup>

<sup>37</sup> See Sarabdeen Jawahitha, Mohamed Ishak & Mohamed Mazahir, *E-Data Privacy and the Personal Data Protection Bill of Malaysia*, 7 J. APPLIED SCI. 732, 740 (2007).

<sup>38</sup> See, e.g., Zuryati Mohamed Yusoff, *The Malaysian Personal Data Protection Act 2010: A Legislation Note*, 9 N.Z. J. PUB. & INT'L L. 119, 133 (2011).

<sup>39</sup> This document is accessible at: <http://statutes.agc.gov.sg/aol/download/0/0/pdf/binaryFile/pdfFile.pdf?CmpId:51ad3f3a-ae52-4a17-9a26-4b08ca7f88a4>.

<sup>40</sup> See Greenleaf, *supra* note 9, at 3.

<sup>41</sup> The limitation of the efficacy of the Act to commercial transactions was not in the first Bill.

<sup>42</sup> E.g., Munir, *supra* note 8, at CXXVII.

<sup>43</sup> See Ismail, *supra* note 16, at 110.

Although the exclusion of credit reference agencies from the application of the P.D.P.A. has been criticized since the individuals may lose in the process of collection and sharing of the personal information by these companies, according to Deputy Finance Minister Datuk Dr Awang Adek Hussin, these companies will be monitored by the Companies Act and the P.D.P.A. 2010.<sup>44</sup> However, the scope, features and adequacy of the credit reference agencies to protect personal data of individuals which typically constitute important information, is out of the scope of this research. Malaysian data processors are not subject to the P.D.P.A. and only data users are responsible. This will affect the adequacy requirement provided under Article 25 of the European Union Directive. It is also inconsistent with the EU General Data Protection Regulation [hereinafter G.D.P.R.]. The legal status of anonymous data is a challenging issue under the P.D.P.A, since it remains unclear whether the P.D.P.A. applies to such data. These issues will be analyzed under the definition of the personal data.

P.D.P.A. does not recognize extra territorial jurisdiction. In fact, the P.D.P.A. does not apply to the personal data of Malaysians that have been processed and used abroad. However, it has been suggested to include the phrase “personal data of Malaysians” under Section 3(2) on data processed abroad, in future amendments to the Act. Secondly, the term “intended” is not precise since the mere intention of further processing in Malaysia will not change the legal status of a foreign company to fall under the application of the P.D.P.A.. In fact, by virtue of mere intention, the P.D.P.A. will not apply to a foreign jurisdiction, as the P.D.P.A. does not recognize extra territorial jurisdiction, and it does not have any extraterritorial enforcement mechanism. Hence, it is suggested to amend this provision by omitting the phrase “is intended”.

The Commissioner is also not empowered under the P.D.P.A. in line with his extensive duties. On the other hand, he is not answerable to the Parliament. This may be considered as a barrier against recognition of Malaysia as a safe country.<sup>45</sup> Zuryati argues that the reason why the Commissioner is not answerable to the Parliament is due to the doctrine of separation of powers under the Malaysian Constitution.<sup>46</sup> However, in most countries, the Commissioners are independent bodies and they are answerable to the parliaments.

---

<sup>44</sup> See Yusoff, *supra* note 38, at 124.

<sup>45</sup> Independence of data protection authorities plays a key role in complete execution of the data protection laws around the world especially in Europe. See generally Laima Jančiūtė, *European Data Protection Board: A Nascent E.U. Agency or an “Intergovernmental Club?”*, 10 INT’L DATA PRIV. L. 57, 57-75 (2020); Philip Schütz, *Accountability and Independence of Data Protection Authorities — A Trade-Off?*, in *MANAGING PRIVACY THROUGH ACCOUNTABILITY* 233, 233-60 (Daniel Guagnin et al. eds., 2012); Graham Greenleaf, *Independence of Data Privacy Authorities (Part II): Asia-Pacific Experience*, 28 COMPUT. L. & SEC. REV. 121 (2012); Alexander Balthasar, *Complete Independence of National Data Protection Supervisory Authorities-Second Try: Comments on the Judgment of the C.J.E.U. of 16 October 2012, C-614/10 (European Commission v. Austria), with Due Regard to Its Previous Judgment of 9 March 2010, C-518/07 (European Commission v. Germany)*, 9 UTRECHT L. REV. 26, at 26 (2013).

<sup>46</sup> See Yusoff, *supra* note 38, at 128.

The 23rd International Conference of Data Protection Commissioners in September 2001 Paris, provided for “Criteria and Rules for Credentials Committee and the Accreditation Principles”.<sup>47</sup> According to its accreditation principles, a data protection commissioner must be a public body to be independent and empowered legally and practically. Asia Pacific Privacy Authorities has also set similar requirements for the Commissioners, in order to fulfill the above mentioned accreditation principles. There is a question as to whether the personal data protection Commissioner of Malaysia is subject to the Act. In some countries, like the United Kingdom, Canada and New Zealand, the privacy regulators have displayed a privacy notice in their websites. It seems that the Malaysian Commissioner Office is a department under the Ministry, and moreover, the Commissioner’s Office does not collect personal data for economic purposes. However, a long time after the establishment of the Commissioner’s Office website, they have displayed a short, incomplete and vague privacy policy which is mostly regarding the use of the website.

The limitation of the P.D.P.A. to the private sector, and private sectors with respect to commercial transactions, can be regarded as defeating its purpose. Since there are many legal debates on the scope of the Federal and State government, there is a serious need to survey the laws and regulations to define the limits of the Federal and State Government. Perhaps there are some executable solutions before the amendments of the Act. It would be most helpful to follow the Singaporeans’ mechanism to enumerate the authorities and departments that fall under the category of the Federal and State government through an order issued by the Commissioner. Furthermore, implementation of a code of practice on privacy protection to be applied by the Federal and State governments may reduce these concerns.

## REMARKS

Nowadays, data protection is a global concern, and Malaysia is not an exception. Under the data protection law, it is an individual’s discretion to allow the data users to collect his/her data or not. If an individual consents, then he/she has the control right over his/her personal data during the processing stages. Although the Malaysian government has initiated the data protection legislation timely, the broad limitations provided under

---

<sup>47</sup> Amended in the 24<sup>th</sup> International Conference of Data Protection and Privacy Commissioners, September 2002, Cardiff (UK).

the P.D.P.A., along with the long time interval between drafting of the Bill, enactment and the late enforcement, have made the law problematic.

One of the most debatable and questionable parts of the P.D.P.A. is its application. The P.D.P.A. applies to the Malaysian private data users, or the data processed in Malaysia merely for the purpose of commercial activities. The P.D.P.A. has provided for total and partial exemptions. The Federal and State Governments, non-commercial activities, personal, family or household affairs, recreational purposes, credit reporting agencies, and information being processed outside Malaysia are exempted from the P.D.P.A. application.

These broad and vague total and partial exemptions were criticized as serious defects of the P.D.P.A. especially when compared to the EU approach. The P.D.P.A. has a very limited scope, which will eventually result in a weak personal data protection mechanism. Even if we forget about the explicit exclusion of the government, there are many exemptions, which, in practice, could exempt the government from certain principles.<sup>48</sup> For example, it seems that the exclusion of non-commercial activities from the application of the P.D.P.A. was another attempt to exclude the government. In the absence of any definition, it is highly suggested that the Minister or the Personal Data Protection Commissioner issue a clarification guideline defining the boundaries of the Federal and State Governments under the P.D.P.A.. Moreover, there is no blanket exemption from the security principle, data integrity principle, and retention principle for those broad partial exemptions.

The P.D.P.A. applies to private companies and for commercial activities only. Again, the definition and examples of commercial activities and non-commercial activities are another defect of the P.D.P.A. in practice. Moreover, the lack of any compensation for the victims of data breach and the lack of administrative fine to be applied by the Commissioner, are other shortcomings of the Act. While the popular approach all around the world is the independence of the commissioners, the Malaysian Commissioner is not independent under the P.D.P.A.. He must report to the Minister and is not accountable to the Parliament.

The Article 29 Working Party, which was an EU advisory body until the enforcement of the G.D.P.R. on 25 May 2018, has also provided for the adequacy requirements in its Working Paper-12. Based on these requirements, Malaysia lacks the adequacy criteria to be recognized as a safe country, although it holds some of those factors. According to the Working Party, a data protection law must apply to all organizations and individuals; however, the P.D.P.A. has excluded the Federal and State

<sup>48</sup> See Personal Data Protection Act, § 45 (2012).

Governments. Moreover, the law must apply to all kinds of processing, while the P.D.P.A. only applies to commercial transactions. An independent authority must monitor and supervise the compliance with the law; however, the Commissioner is not independent under the P.D.P.A.. Finally, the law must contain both compensation and sanctions, but the P.D.P.A. lacks any civil remedy mechanism.<sup>49</sup>

It is recommended that the enforcement of the G.D.P.R. must be considered by the Malaysian legislature in order to amend the P.D.P.A. provisions in line with the new technologies. However, a faster and an easier method is to include such new mechanisms under the Ministerial Orders. This will not affect the important function of the Commissioner to provide interpretations and guidelines and promote the P.D.P.A. through different training programs for both private sector and citizens. The development of data breach notification, appointment of data protection officer, compensation mechanism as well as data protection Impact Assessment would ultimately strengthen the adequacy and functions of the P.D.P.A..

---

<sup>49</sup> For more information on adequacy test issues see Edwin Lee Yong Cieh, *Limitations of the Personal Data Protection Act 2010 and Personal Data Protection in Selected Sectors*, in BEYOND DATA PROTECTION 65 (Noriswadi Ismail & Edwin Lee Yong Cieh eds., 2013); Paul. M. Schwartz, *Global Data Privacy: The E.U. Way*, 94 N.Y.U. L. REV. 771 (2019); Alex Boniface Makulilo, *Data Protection Regimes in Africa: Too Far from the European "Adequacy Standard"?*, 3 INT'L DATA PRIV. L. 42 (2013); Alex Boniface Makulilo, *One Size Fits All: Does Europe Impose Its Data Protection Regime on Africa?*, 37 DATENSCHUTZ UND DATENSICHERHEIT 447 (2013).