Malaysia: ASEAN's first data privacy Act in force

Graham Greenleaf, Professor of Law & Information Systems, University of New South Wales

(2013) 126 *Privacy Laws & Business International Report*, pgs. 11-14, December 2013

Contents

Malaysian Ministers periodically since 1998 announced their intentions to introduce comprehensive data protection legislation. In 2010 the *Personal Data Protection Act 2010* (PDPA) was enacted, but not brought into force. A new Personal Data Protection Department was created to oversee the implementation of the Act in 2011. It was not until 15 November 2013 that the Act was brought into force and Abu Hassan Ismail (previously Director-General of the Department) was appointed as Personal Data Protection Commissioner. A number of Regulations came into force on the same day.[1] Data users have three months to 15 February 2014 to comply with Act and Regulations. This will make it the first data privacy Act in the ASEAN region to be fully in force. This article analyses the main features of the new Act.

The limited scope of the PDPA

The PDPA can only be said to cover part of the private sector, and only then subject to many exceptions, particularly where any State-related activities are concerned. Within its scope it will be valuable, but the narrow scope must always be kept in mind.

Meaning of 'personal data'

The definition of 'personal data' in the PDPA has a conventional starting point in that it is based on any information which identifies a person, directly or indirectly, from information held by data user.[2] It explicitly includes sensitive personal data (defined separately), and expressions of opinion about the data subject. However, the definition also requires that the information satisfy one of three conditions, which can be summarised as: it is being processed by automatic means, or recorded with that intention; or it is recorded manually as part of a set of structured information, or with that intent.[3] Almost all collection of personal data for inclusion in automated or manual record-keeping systems will therefore be included. Any processing of identifying data by automated means, even if it cannot be subsequently retrieved, will be included.

Limitation to commercial transactions

The Act applies only to 'any personal data in respect of commercial transactions'.[4] The definition of personal data also restricts it to 'information in respect of commercial transactions'.[5] 'Commercial transactions' are defined broadly to mean 'any transaction of a commercial nature, whether contractual or not' and that this 'includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance'.[6]

The PDPA includes the usual exemption for 'personal, family and household affairs'[7] but the limitation to 'commercial transactions' will also exclude the non-commercial affairs of churches, educational institutions and non-profit organisations. It should also exclude information about conduct in government affairs. There is no 'small business exemption', unlike in Australia or Japan.

---

1 Personal Data Protection Regulations, 2013 (PDPA Regs); see later for other Regulations and Orders.

2 PDPA, s 4, definition of 'personal data'.

3 PDPA, s 4, definition of 'personal data', conditions (a)-(c).

4 PDPA, s 2.

5 PDPA, s 4, definition of 'personal data'.

6 PDPA, s 4, definition of 'commercial transactions'.

7 PDPA, s 45(2).

Credit reporting business carried out by a credit reporting agency is exempt and is subject to separate legislation.

Exclusion of the public sector and 'regulatory functions'
The largest omission from the scope of the PDPA is that it 'shall not apply to the Federal and State Governments' (s3(1)). However, the exact boundaries of this exclusion are not clear from the PDPA or interpretation legislation,[8] and further statutory interpretation (beyond the scope of this introduction) is required. It is likely that government-owned trading companies would fall outside the meaning of 'Governments', as would companies carrying out government business under contract. Such bodies would have to comply with the PDPA in their 'commercial activities'.

There is a very broad exemption under section 45(2)(e) from most of the Principles for any processing by commercial organisations 'for the purpose of discharging regulatory functions' where application of the Act would be likely to prejudice those functions.[9] This may be used to exempt some government-owned companies, and other companies, from some aspects of the Act.

The necessary approach is to first determine whether an entity is to be regarded as 'government', in which case the PDPA will not apply even if it is carrying out commercial activities. If it is not a 'Government' entity, then the question of 'commercial activities' comes into play, and then the possible exemption under section 45(2)(e).

A limited media exception
Processing for the purpose of publishing 'journalistic, literary or artistic material' is exempted (except from the Security Principle), but only where the data user reasonably believes that (a) the publication would be in the public interest (taking into account the 'special importance of public interest in freedom of expression'), and (b) compliance with a particular Principle or provision is 'incompatible with the journalistic, literary or artistic purposes'.[10] This is not a blanket 'media exemption' but a carefully written partial exemption, and one which will be complex for the media, Commissioner and courts to apply. It is important that this Act should not unduly restrict freedom of expression in Malaysia.

Other exemptions, including Ministerial orders
There are other broad exemptions in section 45 for processing of personal data for specified purposes: for prevention of physical or mental harm, for statistical and research uses that do not produce identified outputs, and in connection with court processes. These are not blanket exemptions from all Principles, and typically do not provide exemptions from the Security, Data Integrity and Retention Principles. In addition, there are lengthy lists of exemptions from specific Principles, particularly Disclosure. Finally, the Minister may, upon the recommendation of the Commissioner, exempt a data user or class of data users from any of the Principles or other provisions of the Act.[11]

Obligations only on data users, not data processors
Obligations under the PDPA are imposed only on 'data users', defined as 'a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data'.[12] The definition expressly excludes a 'data

[8] Interpretation Acts 1948 and 1967

[9] PDPA s 45(2)(e).

[10] PDPA, s 45(2)(f)).

[11] PDPA, s 46.

[12] PDPA, s 4, definition of 'data user'.

processor' from its scope, defined as a 'person, other than an employee of the data user, who processes the personal data solely on behalf of the data user, and does not process the personal data for any of his own purposes.[13] If a data processor starts to process the data for his own purposes (for example, by using or disclosing it, or storing it after it was supposed to be deleted), then the processor becomes a data user at that point, with the liability imposed by the Act.

Conclusions concerning the scope of the Act

The cumulative effect of all of these different types of limitations is that Malaysia's PDPA has a very narrow scope, which can perhaps be summarised as 'the systematic use of personal data arising from commercial transactions in some other commercial transactions (not involving government), subject to numerous exceptions both stated in the Act and subject to potential expansion by the Minister'. However, some uncertain aspects of the apparent exclusions of government from the Act, and the meaning of 'commercial transactions', create latitude for potentially surprising interpretations of the scope of the Act by the Commissioner and the courts.

Seven Principles plus data subject rights

The Act's seven Personal Data Protection Principles in sections 5-12 are more strongly influenced by the EU data protection Directive than by the OECD Guidelines or APEC Framework. There are also what are in effect additional principles in Part II Division 4 'Rights of Data Subject'.[14] Many exceptions to the principles are also provided throughout the Act. The Regulations also now add more detail to these obligations and rights. All of these aspects are now discussed together.

The 'general principle' – processing with consent

The general principle in section 6 is that data users must not process personal data unless the data subject has given his consent to the processing. 'Processing' has the broadest possible meaning,.[15] Processing without consent is then permitted in six situations, three of which concern the processing agreed to by the data subject or to protect the data subject's vital interests, and the other three concern processing for the purposes of carrying out of the legal obligations of the data user, the functions under any law of any third party, or the administration of justice.[16] These exceptions do not apply to sensitive personal data. Regulations provide considerable detail on what is required for consent:[17] it must be in a form recorded and maintained; each requirement for consent must be presented separately ('unbundling'); onus of proof is on the data user. Such requirements are otherwise only found in Asia in Korea's law.

Other general processing limitations – Lawfulness, necessary and 'not excessive'

Section 6(3) sets out three other general limits on processing: a lawful purpose directly related to an activity of a data user; processing necessary for or directly related to that purpose; and personal data 'adequate but not excessive in relation to that purpose'. Given the breadth of the meaning of 'processing', these limits must be considered concerning all uses of personal data.

---

[13] PDPA, s 4, definition of 'data processor'.

[14] PDPA, s 38, s 42 and s 43 respectively.

[15] PDPA, s 4, definition of 'processing'.

[16] PDPA, s 6(2).

[17] PDPA Regs, s 3.

Collection and notice principles

Data users must obtain data subject consent to processing, and give 'written notice' of purpose whenever data is collected, at least before use for related purposes or disclosure.[18] Regulations specify the contact details that must be given.[19]

Use and disclosure principles

Personal data may only be used with consent, or in accordance with one of the exceptions where consent is not required for processing. Personal data may only be disclosed for purposes 'directly related' to the purpose of collection,[20] or to 'the class of third parties' to whom the data user has given notice that 'may disclose' the data.[21] Such notice can be a blank cheque for data users to disclose personal data to anyone they choose, provided they make a general statement about the possibility of disclosure. However, the data user will still have to establish that such notice constitutes the data subject's implied consent to process the data, or be able to rely on one of the exceptions allowing processing without consent.[22] Data users must maintain a list of such disclosures (logging) for 'directly related' purposes,[23] but not where disclosures are made under the exceptions to section 6.

These restrictions on disclosures by data users are backed up by offences which are committed by third parties who collect, or disclose, or sell personal data held by a data user, unless they can show that they acted under conditions justifying their acts.[24]

Sensitive personal data

'Sensitive personal data' appears to have a broad definition (including health, beliefs and offences), but the definition requires that it be 'personal data,'[25] which limits it to 'information in respect of commercial transactions'. The processing of sensitive personal data requires 'explicit consent' (which suggests that 'consent' by itself includes implied consent), or for other exceptions to apply.[26] Among the list of very broad exceptions to the consent requirement are that the use is necessary 'for the exercise of any functions conferred on any person by or under any written law' or 'for any other purpose as the Minister thinks fit'. This provision could be abused by the Malaysian state (which is in effect exempt from the legislation) whereas those who attempt to raise allegations of criminality or discuss other sensitive issues could be prosecuted if they fall outside the media exemptions.

Security principle

The Security Principle requires data users to 'take practical steps', having regard to six specified security factors.[27] Data users are required by Regulations to have security policies which comply with the 'security standard' set periodically by the Commissioner.[28] They must also ensure that any

---

[18] PDPA, sections 6-7.

[19] PDPA Regs, s 4.

[20] PDPA, s 8(a).

[21] PDPA, s 7(1)(e) and s 8(b).

[22] PDPA, s 6.

[23] PDPA Regs, s 5.

[24] PDPA, s 130.

[25] PDPA, s 4 defintion 'sensitive personal data'.

[26] PDPA, s 40.

[27] PDPA, s 9.

[28] Personal Data Protection Regulations, 2013, s 6.

data processors acting on their behalf comply with those policies. The security principle is not included in many of the exemptions in Part III, so it applies to a much broader range of data than the other principles, and has additional importance.

Data retention principle and rights to block processing

Personal data cannot be retained for longer than the fulfilment of the purposes for which it is legitimately processed, and it is the data user's responsibility to ensure that the data is then 'destroyed or permanently deleted'.[29] Data users must comply with any 'retention standard' that the Commissioner may prescribe.[30]

Data subjects can also withdraw consent to the processing of their data at any time and data users must comply.[31] It must be assumed that this is subject to the exceptions to section 6 where consent to processing is not required. Data subjects may also give a data user a 'data subject notice' requesting cessation of processing, or processing not to commence, for a specific period or for a specific purpose, if (for reasons stated) the processing is likely to cause substantial and unwarranted damage or distress to him or another person.[32] The enforcement procedures are discussed below.

Data integrity principle

The data integrity principle is comprehensive: 'A data user shall take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed'.[33] Data users must comply with any 'data integrity standard' that the Commissioner may prescribe.[34]

Access and correction principle

Data subject have standard rights to access their personal data and to correct it where it is 'inaccurate, incomplete, misleading or not up-to-date', except where their requests are refused in accordance with the Act.[35] The grounds for, and procedures relevant to, compliance with or refusal of access and correction requests are set out in sections 30-37. Regulations set out the requirements for acknowledgment of access and correction requests, and the identification details that data users may legitimately require from data subjects (name, address and ID number, unless the Commissioner specifies otherwise).[36]

Where correction of personal data is refused by a data user in relation to an expression of opinion (including an assertion of fact which is unverifiable) then the data subject is entitled to have a note of their opinion of the correct state of affairs added to their file, in such a way that the contested opinion cannot be accessed without the data subject's note also being accessed.[37]

---

[29] PDPA, s 10.

[30] PDPA Regs, s 7.

[31] PDPA, s 38.

[32] PDPA, s 42.

[33] PDPA, s 11.

[34] PDPA Regs, s 8.

[35] PDPA, s 12.

[36] PDPA Regs, sections 9-11.

[37] PDPA, s 37.

International data flows, and processor contracts

Inter-connected issues concerning international data flows (companies or processing from outside Malaysia) are now analysed.

Extra-territoriality

The Act applies to anyone 'established in Malaysia'[38] or who 'uses equipment in Malaysia' (except for transit through Malaysia).[39] Those using equipment in Malaysia must nominate a representative established in Malaysia.[40] The Act has no application to 'personal data processed outside Malaysia', with the interesting exception of where data is 'intended to be further processed in Malaysia'.[41]

Data export rules

Personal data may not be transferred outside Malaysia unless the destination is on a 'whitelist' specified by the Minister, after receiving the Commissioner's advice.[42] The Minister can so specify a place if it has in force a law 'substantially similar' to the Malaysian Act, or the place ensures 'an adequate level of protection … which is at least equivalent to the level of protection' provided by Malaysia's Act. There are exceptions similar to those found in Article 26 of the EU data protection Directive, but some which go considerably further than the Directive, including where 'the data user has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in a manner which, if that place is Malaysia, would be a contravention of this Act'.[43] This applies whether the transfer is to a third party for their own processing purposes, or to a data processor to process on behalf of the Malaysian data user.

Unless the Commissioner takes a strict interpretation of when a data user has 'taken all reasonable precautions and exercised all due diligence', s129 will involve a front door to data exports (the 'whitelist') which appears to be shut, while the back door is wide open to transfers to anywhere, with exporters absolved from any accountability for what goes wrong provided they go through a 'due diligence' ritual. A data user who contravenes s129 will upon conviction be liable to a fine of up to 300,000 Ringitts (US$100,000) or up to two years imprisonment.

Relationship between controller (data user) and processor, and their liabilities

An overseas data processor who acts solely within the terms of the processing contract will not have any liability under the PDPA, because obligations are imposed only on data users. If the overseas processor acts outside those obligation then it becomes a data user with obligations under the PDPA, and the Act will have extra-territorial effect if (and only if) the data is intended to be further processed (used in any way) in Malaysia. But this will be of little use to a Malaysian data subject if it is necessary for them to take action against a data processor located overseas. Although the Malaysian-based data user is only liable for the actions of the overseas processor if those actions are 'authorized' within the terms of the processing contract, that may in many instances give data subjects an action in a Malaysian court against a Malaysian data user.

Data imports and an 'outsourcing exemption'

If personal data is imported into Malaysia for the purpose of processing on behalf of an overseas company by a Malaysian company, the Malaysian company is a data processor, not a data user, and

---

[38] PDPA, s 2(2), with s 2(4) defining the circumstances under which business entities are 'established in Malaysia'.

[39] PDPA, s 2(2).

[40] PDPA, s 2(3).

[41] PDPA, s 3(2).

[42] PDPA, s 129.

[43] PDPA, s 129(3)(f).

therefore does not have liabilities under the Act. Whether the overseas company can be classified as a data user depends on whether the company is 'established in Malaysia', because it is unlikely that it can be said that it 'uses equipment in Malaysia'.[44] It seems, therefore, that personal data sent to Malaysia for processing benefits from an 'outsourcing exemption'. This exemption is likely to undermine any attempt by Malaysia to achieve adequacy status in relation to the EU, and is likely to complicate Malaysia's position in relation to data exports from other countries whose laws include data export restrictions.

Personal Data Protection Commissioner and Appeal Tribunal

Malaysia now has a Personal Data Protection Commissioner, and a separate Department established to administer the Act. The Commissioner is appointed for up to three years, but is not independent: he or she may be dismissed by the Minister, who only needs to 'state the reason'; 'the Commissioner shall be responsible to the Minister'; and 'the Minister may give the Commissioner directions of a general character consistent with the provisions of the Act'.[45] This lack of independence may be an impediment to accreditation from the International Data Protection and Privacy Commissioners meeting or the Asia Pacific Privacy Authorities (APPA). The Act provides the Commissioner with a normal range of functions and powers.[46] The Commissioner is required to provide reasons for any decisions he makes, upon request by any person aggrieved by such a decision[47] (typically a data subject or data user).

Any decisions by the Commissioner may be appealed to an Appeal Tribunal, including questions of registration of data users, registration of codes of practice, issuance of enforcement notices, and even 'the refusal of the Commissioner to carry out or continue an investigation initiated by a complaint'.[48] The Minister appoints the Appeal Tribunal of at least three members,[49] but has not yet done so. There is no right of appeal to the courts from a decision of the Appeal Tribunal.[50]

Registration of data users

Registration of specific classes of data users may be required by the Minister on the recommendation of the Commissioner.[51] The Minister made such regulations on the day the Act came into force, both to specify the classes of data users required to register,[52] and the procedure for registration.[53] Existing data users in classes requiring registration have three months to register from 15 November 2013.[54] The classes of data users required to register are such that they cover most significant data users. Registration will cost between 100-400 Ringitts (US$30-130), depending on

---

[44] PDPA, s 2(2).

[45] PDPA, sections 53-59

[46] PDPA, s 48 and s 49.

[47] PDPA, s 94.

[48] PDPA, s 93.

[49] PDPA, s 85.

[50] PDPA, s 99.

[51] PDPA, s 14.

[52] Personal Data Protection (Class of Data Users) Order 2013

[53] Personal Data Protection (Registration of Data User) Regulations 2013

[54] PDPA, s 146.

the type of business entity, possibly annually. Failure to register or renew may result in fines of up to 250,00 Ringitts (under US$90,000).[55]

In summary, the classes of data users requiring registration are:[56] licensees under communications and postal laws; banking and financial institutions; insurers; licensed health care and pharmacy providers; tourism and hospitality service operators, and tourist accommodation providers; aviation transport providers; private educational institutions; licensed direct selling organisations; companies or partnerships carrying on business as lawyers, auditors, accountants, engineers or architects; those conducting retail or wholesale dealings under the Control of Supplies Act 1961; private employment agencies; various categories of housing developers; and named utilities. A very wide range of Malaysian businesses are therefore required to register, and they appear to be primarily those who would hold substantial amounts of personal information.

Enforcement provisions

The PDPA is unusual is that prosecution of offences is almost the only significant means by which the Act can be enforced, except for an injunction-like procedure by the Commissioner.

Offences

Data users who breach one of the seven Principles in sections 6-12 commit an offence which can on conviction result in a fine of 300,000 Malaysian Ringitts (nearly US$100,000) or two years imprisonment.[57] Further offences can be committed by failure to comply with various 'rights of the data subject'.[58] Contravention of various regulations requiring obtaining consent, or failure to adhere to the various standards set by the Commissioner can also result in similar penalties.[59] In summary, failure to comply with the substantive obligations set out in the Act generally constitutes an offence, no matter where those obligations are located. Prosecutions must be by or with the written consent of the Public Prosecutor,[60] and are within the jurisdiction of a Sessions Court,[61] one of the subordinate courts. As criminal offences, the normal provisions for appeal under Malaysian law will apply.

Enforcement notices and directions

If the Commissioner, after investigation, considers that a data user is (currently) contravening the Act, or has done so in the past and is likely to continue or repeat doing so, then the Commissioner can issue an enforcement notice requiring the contravention to be remedied.[62] Failure to comply with an enforcement notice is an offence, with conviction resulting in a fine of up to 200,000 Ringitts.[63] There is a right of appeal against issuance of an enforcement notice to an Appeal Tribunal (Pt VII). There is no right of appeal against non-issuance of an enforcement notice, which seems somewhat unfair to data subjects, and surprising since there is a right of appeal against the Commissioner's failure to investigate a complaint (s93). The reliance on enforcement notices is less

---

55 Personal Data Protection (Registration of Data Users) Regulations 2013

56 Class of Data Users Order, Schedule

57 PDPA, s 5(2).

58 PDPA, respectively s 37(3), s 38(4), s 40(3), and s43(5).

59 Personal Data Protection Regulations, 2013, s 12, concerning sections 3(1), 6, 7 and 8 of those Regulations.

60 PDPA, s 134.

61 PDPA, s 135.

62 PDPA, s 108(1).

63 PDPA, s 108(8).

of a problem than in Hong Kong's law, at least in theory, because under Malaysia's PDPA breaches of principles are in themselves potential offences.

Blocking of processing following 'data subject notices'
A data subject may give a notice to a data user requiring processing of personal data to cease, or not to begin, on the basis that the processing 'is causing or is likely to cause substantial damage or substantial distress to him or to another person' and 'the damage or distress is or would be unwarranted'.[64]

Inspections
The Commissioner has powers to inspect data user's systems.[65] Data users are required to keep records of 'any application, notice, request or any other information relating to personal data, and the Commissioner can determine how it will be kept.[66] Regulations specify what the Commissioner may require a data user to provide on such an inspection, including records of consent to processing, the notices issued to data users, the list of disclosures to third parties, and the records of compliance with various standards issued by the Commissioner.[67]

A deficient 'enforcement pyramid'
Although the provisions concerning offences and enforcement notices are comprehensive, and involve rights of appeal, there are significant deficiencies in the PDPA's 'enforcement pyramid'. First, there are no provisions by which complainants may seek compensation for damage from the Commissioner or a court. Nor are there provisions for remedies such as apologies, or restoration of services, or injunctions to prevent breaches from occurring (except for the section 42 'data subject notice' procedure). No matter how diligent a privacy Commissioner may be, if they do not have the necessary enforcement tools, there are severe limits to what they can achieve.

Evaluation – An Act of uncertain effectiveness

While the PDPA has many deficiencies, this data privacy legislation will be a significant step forward for Malaysians. In the hands of a Commissioner committed to privacy protection, and a government which does not impede this, much will be achievable. However, the range of enforcement methods is insufficient: there are no provisions by which complainants may seek compensation or most other remedies.

If the Act is well managed and gains credibility, Malaysian politics may deliver further improvements to it in future, particularly in expansion of scope to cover the public sector, and provision of some avenue for compensatory damages. For Malaysians to be able to focus on real issues in data protection, because of the existence of this Act, will inevitably increase the demand for better protection.

---

[64] PDPA, s 42.

[65] PDPA, sections101-103.

[66] PDPA, s 44.

[67] Personal Data Protection Regulations, 2013, s 14,