

University of New South Wales
University of New South Wales Faculty of Law Research Series
2012

Year 2012

Paper 14

ASEAN's 'New' Data Privacy Laws:
Malaysia, the Philippines and Singapore

Graham Greenleaf*

*University of New South Wales, g.greenleaf@unsw.edu.au

This working paper is hosted by The Berkeley Electronic Press (bepress) and may not be commercially reproduced without the permission of the copyright holder.

<http://law.bepress.com/unswwps-flrps12/art14>

Copyright ©2012 by the author.

ASEAN's 'New' Data Privacy Laws: Malaysia, the Philippines and Singapore

Graham Greenleaf

Abstract

In the first quarter of 2012, the ASEAN region (Association of South East Asian Nations) has become the most active region in the world for new privacy developments. None of the Bills in Malaysia, the Philippines or Singapore is yet a law, but they all could be within 2012. They have very different strengths and weaknesses in the protections they give to data subjects, and present differing compliance challenges for businesses.

Malaysia's Personal Data Protection Act of 2010 has not yet been brought into force, primarily because the government has not appointed a Personal Data Protection Commissioner as required by the Act. The Malaysian government has now indicated it is considering bringing the Act into force without a Commissioner. This article considers whether such a move could result in serious enforcement.

The Philippines Senate passed the Data Privacy Act of 2011 on 20 March 2012, but the Senate Bill differs from House Bill 1554 passed in 2011. There must now be a bicameral conference committee to 'reconcile' the versions of the two houses, and then the reconciled version will be sent to the President for signature after its passage by both Houses. No timetable has been set. This article examines the main features of the Senate Bill, including its attempt to exempt outsourcing of foreign personal data, which may result in a Pyrrhic victory for outsourcers if it makes it impossible for the European Union to find that Philippines law is 'adequate'.

Singapore's Ministry of Information, Communications and the Arts (MICA) has issued a draft Personal Data Protection Bill, and further consultation paper, while calling for submissions. The data protection principles in the draft Bill are to

OECD or better standard in relation to access, correction, data quality, security, notice and deletion/de-identification. However, it does not have specific provisions restricting data exports. Contrary to suggestions in the previous consultation paper, the Bill does not include special protection for some forms of sensitive data; nor an 'opt-in' by industry sectors for its more onerous principles; nor an 'opt-out' for industry sectors (with DPC permission) from some of the basic principles. The draft Bill therefore appears to be a minimal version of a 'normal' data privacy law, rather than the somewhat derisory version promised by the earlier consultation paper.

The article highlights some interesting comparisons: Whereas Malaysia seems intent on abandoning its enacted (but not appointed) data protection authority, both the Philippines and Singapore are going ahead with enacting laws establishing DPAs. Whereas the laws in neither Singapore or Malaysia will cover the public sector, the Philippines law will do so. The Malaysian law does not seem to include a means for complaints to make claims for compensation, but both the Singaporean and Philippines laws do so. ASEAN member countries have agreed to develop 'best practices / guidelines' on data protection (but not to legislate) by 2015, as part of their commitment to establish an integrated ASEAN Economic Community (AEC) by 2015. It is an area to watch.

ASEAN's 'new' data privacy laws: Malaysia, the Philippines and Singapore

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

Privacy Laws & Business International Report, Issue 116: 22-24, April 2012

In the first quarter of 2012, the ASEAN region (Association of South East Asian Nations) has become the most active region in the world for new privacy developments. None of the Bills in Malaysia, the Philippines or Singapore is yet a law, but they all could be within this year. They have very different strengths and weaknesses in the protections they give to data subjects, and present differing compliance challenges for businesses.

Malaysia: Retreat to advance

Malaysia's *Personal Data Protection Act* of 2010 has not yet been brought into force, primarily because the government has not appointed a Personal Data Protection Commissioner as required by the Act. However, in February 2012 Malaysia's Information Communications and Culture Minister Datuk Seri Dr Rais Yatim indicated that the Act may be brought into force as early as June (though there is no commitment to do so), subject to establishment of a new Personal Data Protection Department to administer it (a Director-General has been appointed). There appears to be no intention to appoint a Commissioner, so the question arises of whether this can be serious data protection legislation, given that most of the legislation presupposed a Commissioner.

The Act has previously been analysed in this Report¹. It applies only to commercial activities in the private sector (but not credit reporting, for which there is a separate Act), exempting the public sector and non-profit activities in the private sector. It has a carefully written partial exemption for media activities (although there are considerable dangers of repressive State use of the sensitive information provisions against non-media parties), and many other specific exemptions.

The Act's seven Personal Data Protection Principles are influenced strongly by the EU data protection Directive rather than by the OECD Guidelines or APEC Framework. The EU-style starting point is that processing of personal data (including collection) requires consent, subject to many exceptions, and the Directive's influence is seen in other principles: the right of data subjects to withdraw consent to processing; a right to prevent processing likely to cause damage or distress; and the right to prevent processing for the purposes of direct marketing. There is a restriction on data exports. However, the limits on use and disclosure are weak. There are numerous exemptions throughout.

What enforcement will be possible?

Section 5(2) provides that any breach of any of the seven Personal Data Protection Principles by a data user is an offence which can on conviction result in a fine of 300,000 Malaysian Ringgits (nearly US\$100,000) or two years imprisonment. Prosecutions must be with the written consent of the Public Prosecutor, and are before a Sessions Court. It is very unusual for a data privacy law to

¹ Munir, A B 'Malaysia introduces personal data protection Bill' *Privacy Laws & Business International Newsletter*, Issue 102, December 2008, p18-19; Greenleaf, G 'Limitations of Malaysia's Data Protection Bill' *Privacy Laws & Business International Newsletter*, Issue. 104, No. 1, pp. 5-7, April 2010, available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2025357>

have criminal prosecutions as its sole means of enforcement. Without a Commissioner, no authority has express power to anyone to receive or investigate complaints. It is difficult to envisage a Department operating an effective system for investigating and resolving complaints with no legislative backing at all. Perhaps it can be done, but it seems more likely that the Malaysian government will seek to amend the Act to replace the Commissioner with a Department. Given the almost complete lack of independence of the Commissioner provided by the Act, it will probably not make much difference. Perhaps the Minister will try to do this by using his powers to issue a simple gazette notice under s144 to modify the Act in whatever way seems 'necessary or expedient for the purposes of removing any difficulties or preventing anomalies in consequence of the coming into operation of this Act'.

The Philippines: A Bill needing reconciliation, and interpretation

The Philippines Senate passed the *Data Privacy Act of 2011*² on 20 March 2012, but the Senate Bill differs from House Bill 1554 passed in 2011. There must now be a bicameral conference committee to 'reconcile' the versions of the two houses, and then the reconciled version will be sent to the President for signature after its passage by both Houses. No timetable has been set. House Bill 1554 is significantly different from this Senate Bill, and much stronger in some of its principles. 'Reconciliation' will be no easy task, and the final Act may differ from what is discussed here. However the purpose of this article is to examine the Senate Bill.

The scope of the Senate Bill covers both the private and public sectors, subject to exemptions for 'personal, family or household affairs', 'journalistic, artistic, literary or research purposes', various aspects of government employment or licensing, for information necessary to carry out government functions, and for research. Rights survive death and may be exercised by the data subject's heirs, an unusual provision.

The Bill has extra-territorial application to 'personal information controllers and processors ... not found or established in the Philippines' but who use equipment located in the Philippines or maintain an office or agency there, provided the information relates to a Philippine citizen or resident, or the entity concerned has a specified link with the Philippines. So it will have broad application to information about Filipinos which is processed overseas.

Exempting (some) outsourcing: Pyrrhic victory?

There is a complete exemption (not found in the House Bill) for 'information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.' So outsourced processing in the Philippines of data collected overseas is exempt, in an apparent attempt to 'protect' the Philippines BPO industry. The problem is that, while this might make it easier to obtain outsourcing contracts from the USA, it would seem to make it impossible for the Philippines to be considered by the EU to provide 'adequate' data protection, since the main purpose of adequacy findings concerns the protection given to data about Europeans. EU outsourcers and their Philippines processors would have to continue to rely on contractual clauses to justify data exports from Europe. For companies in both EU countries and any other countries that have data export restrictions, outsourcing to the Philippines will remain cumbersome.

Can Philippines companies operating call centres for overseas companies utilise this exemption? They do collect information directly from 'residents of foreign jurisdictions' (as is usual in call centre operations). From the wording of the section, it seems they can only utilise the exemption if they collect the personal data 'in accordance with the laws of those foreign jurisdictions'. Otherwise, they will have to comply with the Philippines law. How is a Philippines call centre staffer to know

² The Bill is at <http://www.senate.gov.ph/lisdata/1218710275!.pdf>

how to apply the data collection rules in Australian, UK, or Korean law? This provision will be one major focus of ‘reconciliation’.

Philippines Data Privacy Principles

The purpose of collection must be declared before or as soon as practicable after collection. *Collection is limited* to data which is ‘not excessive’ in relation to purpose (but ‘minimal’ collection is not required). *Subsequent use and disclosure* (and other processing) is prohibited unless the data subject has given express or implied consent, or for various other usual exceptions. There is also an ill-defined and potentially very broad exception where the processing is necessary for the legitimate interests of the controller or third parties to whom the data is disclosed, except where those interests are over-riden by the constitutional rights of the data subject.

Processing of *sensitive data* is prohibited subject to very narrow exceptions, which will not normally allow commercial uses except to establish ‘legal claims’ (which could be interpreted broadly). In addition to the usual categories of sensitive information, the Bill also includes genetic information, information about offences or charges, government ID numbers, and tax or adverse licensing information, and information regarded by law as ‘classified’. Businesses may find these Philippines requirements much stricter than elsewhere. *Data quality* is required in that data must be accurate, relevant and up-to-date relative to purpose.

Security of data is subject to very detailed provisions including requirements of *data breach notification* to the Privacy Commission and to affected data subjects. *Access and notification rights* are quite strong but the *correction* provisions require that the information prior to correction (ie false information) also continues to be provided to any recipients. *Blocking or deletion* of data is required after the completion of the purposes of processing and all related purposes.

A specific ‘*Principle of accountability*’, while poorly worded, appears to make the data controller ‘responsible’ and ‘accountable’ for compliance with the Act, including for when data is disclosed to third parties ‘whether domestically or internationally’. The controller must use ‘contractual or other reasonable means to provide a comparable level of protection’, but whether this means that the controller still has legal liability for any breaches of this protection by the third party remains obscure. If they do not, their ‘accountability’ will usually be worthless to data subjects. There are no express *data export limitations* to countries with inadequate laws (the ‘accountability’ principle operates instead), but the Privacy Commission may have powers to ban exports in some cases (this is uncertain).

A Philippines DPA and its powers

A National Privacy Commission is created, with a Commissioner and two Deputies. Their qualifications and independence are specified in some detail. It has functions of ensuring compliance with the Act, and to investigate complaints, adjudicate, ‘award indemnity’ (compensatory damages), publicise reports of cases, and recommend prosecutions. It can ban processing (temporarily or permanently) that it considers ‘detrimental to national security and public interest’. It can coordinate with overseas privacy regulators and ‘private accountability agents’ and participate in international and regional privacy initiatives, which will facilitate cooperation in APEC processes. It can also approve (or reject) voluntary privacy codes, but the consequences of such approval are not specified. Many breaches of the Principles may also constitute offences, including unauthorised processing. It seems as though actions for damages (‘restitution’) may also be possible via the New Civil Code (ie via the Courts), but only when an offence has occurred.

An ambiguous Bill

This Bill creates a seemingly credible data protection authority, and range of enforcement mechanisms. The principles in the Bill generally implement OECD standards, but often in a weak fashion, such as the very ambiguous restrictions on use and disclosure, and the bizarre interpretation of 'correction'. They add some additional 'European' standards such as deletion rights and protection of sensitive information, but lack 'border control' data export restrictions. They add the post-Directive requirement of data breach notification. The 'accountability' provisions may be strong or weak, the outsourcing exemptions broad or narrow. Interpretation will be crucial to what this law means, if it is enacted like this after 'reconciliation'.

Singapore: Modest protection, potential dangers

Singapore's Ministry of Information, Communications and the Arts (MICA) has issued a draft Personal Data Protection Bill³ and further consultation paper⁴ on the proposals, and indicated that legislation will be introduced to Parliament this year. The draft Bill confirms some of the features foreshadowed in the previous discussion paper⁵, but jettisons others and has some valuable additions.

The draft Bill provides for a Data Protection Commission (DPC), but one with no independence, as its members can be sacked with no reason required. There is an Appeals Board for organisations dissatisfied with DPC decisions. The DPC will have powers to issue orders for an organisation to rectify non-compliance with the DP law, and can require payment of financial penalties for contravention of up to S\$1 million (around US\$1 million), which will help to fund the DPC. The DPC can investigate complaints, but cannot award damages to complainants. It might be able to stop penalty proceedings if a complaint is settled privately, to encourage settlement. However, complainants have a right of private action before a court to obtain injunctions or damages (not mentioned in the previous Discussion paper), but cannot initiate such actions if the DPC has made a decision in relation to the same contravention and appeal rights have not yet been exhausted.

The scope of the draft Bill is complex. It applies to identifiable persons, including to disclosures concerning persons deceased for not more than 10 years. There is limited extra-territorial operation for processing actions with a 'Singapore link'. It does not apply to the public sector. There are exemptions in relation to collection, use and disclose (but not other principles) for news organisations in relation to news activities, but these only apply to organisation declared to be news organisations by the Minister for the purpose of this Act. So there is potential for this legislation to be abused to further limit freedom of speech in Singapore.

The data protection principles in the draft Bill are to OECD or better standard in relation to access, correction, data quality, security, notice and deletion/de-identification. While the principles concerning collection, use and disclosure are based on the purpose of collection (with consent or 'deemed consent') or what 'a reasonable person would consider appropriate' (and gives notice), the substance of these rights is further reduced by lengthy schedules of exemptions for collection, uses and disclosures. The result is very complex. There is no specific provision restricting data exports to countries with inadequate privacy laws. The draft Bill also establishes a Do Not Call Register.

³ Draft Personal Data Protection Bill at http://www.mica.gov.sg/DPbillconsultation/Annex%20D_Draft%20PDP%20Bill%20for%20Consultation.pdf

⁴ Singapore Consultation Paper at <http://app.mica.gov.sg/Default.aspx?tabid=488>

⁵ Discussed in the Singapore section of Greenleaf, G 'Major Changes in Asia-Pacific Privacy Laws: 2011 Survey', *Privacy Laws & Business International Report*, Issue 113: 1, 5-14, October 2011, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2001820

Contrary to suggestions in the previous consultation paper, the Bill does not include special protection for some forms of sensitive data; nor an ‘opt-in’ by industry sectors for its more onerous principles; nor an ‘opt-out’ for industry sectors (with DPC permission) from some of the basic principles. The draft Bill therefore appears to be a minimal version of a ‘normal’ data privacy law, rather than the somewhat derisory version promised by the earlier consultation paper.

The rest of ASEAN: Potential for more legislation

ASEAN member countries have agreed to develop ‘best practices / guidelines’ on data protection (but not to legislate) by 2015, as part of their commitment to establish an integrated ASEAN Economic Community (AEC) by 2015. Vietnam already has most of a data privacy law in its consumer law in force since July 2011⁶, but with no evidence of enforcement as yet. According to its report to the APEC Data Privacy Subgroup meeting in Moscow in January 2012, Vietnam is also formulating a new E-commerce Decree which will have a chapter dedicated to data privacy issues, including regulations on accountability agents, expected to be released by the end of 2012.

Thailand’s draft legislation is still being considered by the new government. Brunei reported to the January APEC meeting that the government is considering development of data privacy legislation for both the public and private sectors. No new developments are known in Indonesia, Cambodia, Laos or Myanmar, but it would not be surprising if some legislative developments occur, in light of the 2015 commitment. Timor Leste’s bid to become an ASEAN member is still being considered.

ASEAN may become one of the world’s most active regions for data privacy legislation, but as yet it is only potential. These Bills demonstrate that a high level of activity in ASEAN is unlikely to result in consistent, or high, levels of protection, but is likely to be a modest advance on the current absence of data privacy laws.



⁶ See Vietnam section in above article.