ASEAN data privacy developments 2014-15

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia

(2015) 134 Privacy Laws & Business International Report, 9-12

From 2010 to early 2014 (from the enactment of Malaysia's law, to when parts of Singapore's law came into force), the countries of ASEAN (Association of South East Asian Nations) were one of the world's most active regions for data privacy developments.[1] During the past year to May 2015, the pace of developments has cooled somewhat, but is still significant in Singapore (particularly data exports), Thailand (new Bills) and Vietnam (detailed enforcement regulations). This article analyses developments for the year prior to April 2015in Singapore, Malaysia, Vietnam, the Philippines, Thailand, Indonesia and Brunei. There have been no significant privacy-related developments during that period in the other four ASEAN states (Cambodia, Lao PDR, Myanmar and candidate member Timor Leste).

Thailand – Junta proposes its own privacy Bill

Thailand's military junta, the National Council for Peace and Order (NCPO), seized power from the elected Shinawatra government in early 2014, ending one of Thailand's longer periods of civilian and democratic government, since 2006. The junta approved a *Data Protection Bill* on 22 July 2014 (the '2014 Bill'), for consideration by the National Legislative Assembly (NLA), a body which it appointed. A Sub-Committee of the NLA was considering legal issues arising from recommendations submitted by various interest groups permitted to make submissions, but apparently did not receive the first of three readings required[2] before assent by the monarch. Full details of the 2014 Bill were not made public,[3] and it is uncertain to what extent it was similar to the Bill that the previous legislature was considering at the time of the coup (the 'Shinawatra Bill').

However, in January 2015, the junta's Cabinet approved a new *Personal Data Protection Bill* (the '2015 Bill')[4] as part of a very controversial package of six e-commerce, broadcasting and cyber-security Bills.[5] The Bills have not yet gone to the NLA. The 2015 Bill proposes to create National Data Protection Committee (NDPC) of up to 10 persons, which is almost certain to have a majority from government and security agencies. The Bill is under the Minister of Digital Economy and Society. Its scope covers both the private and public sectors in theory, but the existing (and

---

[1] For comprehensive discussion of developments prior to May 2014, see Graham Greenleaf *Asian Data Privacy Laws – Trade and Human Rights Perspectives* (OUP, 2014), Chapters 10 – 14, covering the countries of the ASEAN region.

[2] A Bill is then announced in the Government Gazette: see Interim Constitution of the Kingdom of Thailand B.E. 2557 (A.D. 2014) and the NLA's Meeting Regulations B.E. 2557 (A.D. 2014).

[3] Local commentators, who had not obtained the whole Bill, stated that 'The Bill establishes a Data Protection Committee to regulate policies, standards and guidelines regarding the protection of personal data. The Data Protection Committee comprises: 1) a minister; 2) government officers; 3) representatives from the Consumer Protection Board, the Thai Chamber of Commerce and the Thai Bankers' Association; and 4) legal and technology experts appointed by the Prime Minister. The term of the Data Protection Committee is proposed to be three years.' See Dhiraphol Suwanprateep, Nont Horayangura and Pattaraphan Paiboon (Baker & McKenzie, Bangkok) 'National Council for Peace and Order Approves Draft Data Protection Measure' 14 WDPR 39 (29 September, 2014).

[4] [Draft] Personal Data Protection Act (Thailand) (Unofficial English translation by Thai Netizen Network, January 2015) <https://thainetizen.org/wp-content/uploads/2015/01/personal-data-protection-bill-20150106-en.pdf>

[5] The National Broadcasting and Telecommunications Commission (NBTC) Bill, the Cyber Security Bill, the New Computer Crime Bill, the Personal Data Protection Bill, the Digital Economy Promotion Bill, and the Digital Economy Development Fund Bill. Unofficial English translations are at <https://thainetizen.org/2015/01/digital-economy-cyber-security-bills-en/>.

powerless) Official Information Commission (OIC) will handle privacy regulation and complaints concerning the public sector, but apparently without the NDPC's enforcement powers. The Bill has exemptions for uses of data for government 'planning', or criminal investigation, or as required by law. It also exempts publicly available data (s23), and all existing data is excluded from most of the Act (s50). However, there is no exemption in favour of journalism or other aspects of freedom of speech, which is a dangerous absence in Thailand. The Bill has been criticised by business interests for its vague definition of a data controller, which it is feared my result in data processors also being liable for breaches.

The enforcement powers under the 2015 Bill include that the NDPC can prohibit processing, or order remedial actions, and order that data be destroyed (s36). There are numerous offences carrying fines and jail sentences (presumably prosecuted before the courts, not the NDPC) (s43). There are also provisions for civil liability and compensation to data subject for breaches, unless the controller can show that (among other things) they were complying with 'an order of … a government official'. There is also an unusual provision that compliance with this Act makes any actions lawful (s19), apparently irrespective of other laws.

Many provisions in the Bill include the basic OECD privacy principles, with notable exceptions, and some additions. While use and disclosure of personal data must comply with the purpose of collection, such purposes can be changed by either informing the data subject of the change, or by obtaining their consent, 'depending on the circumstances' (s20). This provision is bizarre in not defining what circumstances require consent. A list of categories of sensitive data is given higher protection, but the NDPC can additionally specify as sensitive 'any data which may upset another person's or the people's feelings' (s25). This is a dangerous provision by which the military could make many types of politically contentious data about a person (eg their affiliation with the military or the security services) 'sensitive', so that discussion of them would become a breach of the privacy law.

Access to a person's own personal data can be denied if it affects Thailand's 'security' or 'economy and commerce' or the 'rights and freedoms of another' (with no balancing of the data subject's rights required). Abuse of such vague provisions is likely.

An unusual provision is that the NDPC can issue a 'certifying mark' indicating that a business's practices are compliant with the Act. Although the consequences of this are uncertain, it seems to raise likely conflicts of interests when the NDPC so certifies a business and then has to investigate claims that its practices breach the legislation.

The data export provisions of the Bill prohibit exports of personal data 'to another country whose rules on the protection of personal data is substantively inferior to the standards afforded under this Act' (s27), which can be prescribed by a NDPC 'White List' of such countries. Otherwise, there is a list of exceptions similar to those found in the EU Directive, plus an unusual exception "where it is a transfer to a person who has been granted the mark certifying practice on personal data protection by the Committee, or under the framework of an international co-operation or an international mission." This vague provision (in this unofficial translation) may indicate that the NDPC intends to 'certify' multi-nationals in relation to the privacy protection they provide in any country, and also to provide some way for 'an international co-operation' such as APEC-CBPR (Cross-border Privacy Rules) to be regarded as sufficient to justify exports. It is too brief to give clarity.

Although Thai citizens and responsible businesses would benefit from a well-considered data protection law, there is a strong danger that this ill-drafted Bill has been designed to aid authoritarian rule, as much as to achieve more desirable objectives.

Vietnam – Penalties give clarity to offences

Vietnam's laws dealing with data privacy were previously vague on the sanctions to be applied to breach of various principles, but this is no longer so. The government of Vietnam issued decrees effective January 2014 'providing guidance on sanctions for violations in the information technology and communications (ITC) sector,'[6] implementing Vietnam's 2012 changes to its administrative sanctions regime.[7] The sanctions now provided are low by international standards, but they are precise.

Decree 174[8] stipulates for violations of the Information Technology Law of 2006 and the E-Transactions Law of 2005 fines of up to VND 30 million (US $1,410) apply for failing to have a mechanism to protect users' personal information or actively providing illegal information or personal information.[9] Fines of between VND 10 million (US $470) and VND 20 million (US $940) apply to collecting, processing and using an individual's personal information without his or her consent, and fines of up to VND 30 million (US $1,410) apply to disclosing personal information or other secret information collected from a social network website without prior consent of the relevant organizations and individuals.[10] Various types of failures to respond adequately to network security incidents (including personal data breaches) will also attract similar fines.[11]

There is also a surveillance aspect to Decree 74, because fines of a similar level apply to organisations failing to monitor the electronic information of an organization or individual when so requested by a competent authority or failing to provide personal information of a user involved in terrorist activities or other criminal violations upon the request of a competent authority.[12]

A similar range of offences apply to operators of e-commerce websites. Decree 185[13] provides that Vietnamese authorities may impose fines of more than VND 50 million (US $2,350) and/or revoke the ".vn" domain name of an e-commerce website if its operator is guilty of stealing, using, disclosing, transferring, or selling consumers' personal information in e-commerce without the consent of the consumer, or of deceiving consumers on e-commerce websites.[14] Fines of up to VND 30 million (US $1,410) apply to e-commerce websites failing to safeguard consumers' personal information.[15] Fines of up to VND 30 million (US $1,410) and/or suspension of an e-commerce website for a period of between six and twelve months applies to these violations of personal information: collecting consumers' personal information without their prior consent; setting up a

---

[6] Lee Chung Seck, Minh Tri Quach and Andrew Fitanides (Baker & McKenzie Vietnam) 'Vietnam's New Sanctions for Violations Involving Data Privacy, Data Security, Consumer Protection, E-Commerce, Spam and Social Media' 14 WDPR 23.

[7] Law No. 15/2012/QH13 (20 June 2012) on the Handling of Administrative Violations (Vietnam), replacing Ordinance No. 44/2002/PL-UBTVQH10 (16 July 2002) on the Handling of Administrative Violations.

[8] Decree No. 174/2013/ND-CP (Government of Vietnam, 13 November 2013), Regulating Administrative Sanctions for Violations Relating to Postal Services, Telecommunications, Information Technology, and Radio Frequencies (Vietnam).

[9] Articles 63 and 64, Decree 174 (Vietnam).

[10] Articles 66 and 64, Decree 174 (Vietnam).

[11] Article 71, Decree 174 (Vietnam).

[12] Articles 66 and 65, Decree 174 (Vietnam).

[13] Decree No. 185/2013/ND-CP (Government of Vietnam, 15 November 2013), Regulating Administrative Sanctions for Violations in Commercial Activities and Production, Trade of Counterfeit or Forbidden Goods, and Protection of Consumers' Rights (Vietnam).

[14] Article 82, Decree 185 (Vietnam).

[15] Article 83, Decree 185 (Vietnam).

default mechanism compelling consumers to consent to the sharing, disclosing, or use of their personal information for advertising or other commercial purposes; and using consumers' personal information for other purposes that differ from the use previously announced to the consumers.[16]

Singapore – Enforcement awaited, but Xiaomi under investigation

On 2 July 2014, the data protection provisions of Singapore's *Personal Data Protection Act* 2012 (PDPA) came into force, following an 18 month transition period for companies to prepare for compliance.

Data export regulations

To complete the process, the Personal Data Protection Regulations 2014 (PDPR) were made on 15 May 2014. The most important aspects of the Regulations concern personal data exports. Singapore's approach is very thorough and not easily classified – it is sui generis. The Act requires that data exports should only be to recipients bound by legally enforceable obligations comparable to those found in Singapore, and also includes some elements of extraterritoriality. Regulation 10 specifies that 'legally enforceable obligations' may include laws, contracts, binding corporate rules (BCRs) or 'any other legally binding instrument'. It probably gives individual data subjects few opportunities to protect themselves against unprotected exports, unless an export becomes publicly notorious. However, it does impose obligations on companies which, if not observed, could result in PDPC enforcement action if something goes badly wrong.[17]

Enforcement and Xiaomi

Singapore's Personal Data Protection Commission (PDPC) has been very active in investigating and enforcing the Do Not Call Register provisions of its Act, no in force for over a year. Penalties have included fines of S$29,000 against both a tuition agency, and its director, for sending unwanted SMS messages to persons listed in the Register, and another fine of $$27,000 against a property agent.[18]

Nine months after the data privacy provisions of the Act came into force, no penalties or investigation results have yet been announced. However, since August 2014 the PDPC has been investigating a complaint against Chinese smartphone manufacturer Xiaomi, believed to be the third largest smartphone company after Samsung and Apple. The basis of the complaint is reported to be that a Finnish security firm published the results of their test of a Xiaomi RedMi 1S phone and concluded that on start up the phone automatically sent certain personal data, including information from the user's phone book, to an external server. The complaint was that Xiaomi had disclosed the complainant's personal data without his consent when he used his phone in Singapore, in breach of the Act's disclosure requirements (and possibly the provisions concerning data exports), and as a result he was receiving unsolicited calls from overseas numbers.[19] The PDPC's report on this first case is expected to indicate the approach they intend to take to investigations and use of enforcement powers.

---

[16] Article 85, Decree 185 (Vietnam).

[17] For more detailed analysis, see Greenleaf, G 'Regulations bring Singapore's data privacy law into force' (2014) 130 *Privacy Laws & Business International Report,* 1-4.

[18] Luke Grubb, Chei-Liang Sin & Sally Murphy 'Enforcement of the Personal Data Protection Act in Singapore' (25 February 2015) Latham & Watkins website <http://www.globalprivacyblog.com/privacy/enforcement-of-the-personal-data-protection-act-in-singapore/>

[19] Luke Grubb, Sally Murphy and Kee-Min Ngiam 'Singapore's first data breach?' Latham & Watkins website (21 August 2014) <http://www.globalprivacyblog.com/privacy/singapores-first-data-breach/>

Other consolidating steps

Other aspects of how the PDPA is being brought into force are variously provided by regulations concerning deceased persons, draft Guidelines, and exemptions promulgated by the Monetary Authority of Singapore which illustrate a major weakness of the PDPA. They have a common feature that businesses involved with Singapore need to be aware of considerable regulatory detail or there are considerable risks involved. [20]

The procedure for appeals against directions or decisions by the PDPC has been amended and given considerable detail by an amendment to the 7th Schedule of the Act,[21] and detailed Appeal Regulations.[22] An Appeal Committee will consist of three persons who will decide by majority. The Regulations cover such matters as filing fees (S$600, except in relation to access or correction to an individual own file, where it is only $50), filing and service of process, hearings including forcing attendance of witnesses, and grounds for summary dismissal of appeals. A forward step for transparency of the Act is that the Appeal Panel may decide to publish its decision or any direction.[23] The process provided for is quite formal, but may result in transparency.

The Singapore Infocomm Development Authority was accredited as a member of the International Conference of Data Protection and Privacy Commissioners (ICDPPC) at their meeting in Mauritius in October 2014. This shows that independence from government is no longer a requirement for ICDPPC membership.

Malaysia – In force, with intermittent signs of life

Malaysia's *Personal Data Protection Act*, enacted in 2010, was the first Act in an ASEAN country to come into full force, with data users required to comply with the Act and regulations from 15 February 2014. Malaysia now has a Personal Data Protection Commissioner, Encik Mazmalek bin Mohamad,[24] who administers a Personal Data Protection Department (PDPD) as Director-General,[25] with an establishment of over 40 staff. There is considerable information on the PDPD website (mainly in Bahasa Malay), including a complaint form.[26] No details of any enforcement notices or prosecutions for offences are yet provided.

The PDPD issued in early 2014 a draft set of general guidelines for compliance with the Act,[27] and draft guidelines dealing specifically with the employment relationship,[28] but final guidelines do not seem to have been issued.

---

[20] They are discussed in Greenleaf 'Regulations bring Singapore's data privacy law into force'.

[21] Personal Data Protection (Amendment of Seventh Schedule) Order 2015 (Singapore).

[22] Personal Data Protection (Appeal) Regulations, 2015 (Singapore).

[23] Personal Data Protection (Appeal) Regulations, 2015 (Singapore), Reg. 29.

[24] He was appointed as the new Director General of the Personal Data Protection Department as of 1 October 2014, following the retirement of Haji Abu Hassan Ismail.

[25] Personal Data Protection Department (Malaysia) <http://www.pdp.gov.my/index.php/en/>

[26] Complaint form (Malaysia) <http://www.pdp.gov.my/images/pdf_folder/pdf_borang_aduan_finall_2014.pdf>

[27] PDPD (Malaysia) *Proposal Paper – Guideline on Compliance for Personal Data Protection Act* (No 2/2014) <http://www.foongchengleong.com/downloads/Proposal Paper - Guideline on Compliance for Personal Data Protection Act 2010.pdf>.

[28] PDPD (Malaysia) *Proposal Paper – Guide on the Management of Employee Data Under Personal Data Protection Act (PDPA) 2010* (No 3/2014) <http://www.foongchengleong.com/downloads/Proposal Paper - Guide on the Management of Employee Data Under Personal Data Protection Act %28PDPA%29 2010.pdf>.

The Philippines – Still asleep, with a pretence of protection

Although the Philippines *Data Privacy Act* has been in force since 30 August 2012, this is meaningless because the President of the Philippines has still not appointed a National Privacy Commission (NPC). Only the NPC can make the Implementing Rules and Regulations (IRR) under the Act, and only when that is done are existing businesses and government agencies given one year (or such other time as the NPC specifies) to comply with the Act's requirements.[29] Even some Philippines legislators make the mistake of assuming that the offences created by the Act already apply,[30] but it is hard to see how this can be so when the Act does not yet require any compliance. An attempt by lower house Representative RT Romulo in June 2014 to refer the delay to the Committee on Information and Communications Technology seems to have gone nowhere.[31] Claims that the Philippines has a data privacy law are at this point simply misleading propaganda.

Indonesia – No comprehensive privacy Bill, but corrupt ID system advances

During 2014 there were no significant data privacy developments in Indonesia, including no progress toward a comprehensive data privacy law. However, Indonesia's national electronic ID card scheme continues to advance despite the legislative vacuum concerning privacy, and despite the likelihood of very substantial corruption in its operation. The e-ID card (locally known as the e-KTP project) has been very substantially provided to the more than 170 million eligible recipients (over age 17), but credible allegations (accepted by the responsible Minister) have emerged that fake e-IDs have been manufactured in France and China. With the election of the new government, the Minister suspended further roll-out until January 2015 to allow for an investigation of the situation.[32] New President Joko Widodo has announced separately that Indonesia's migrant workers identification card program (known as the KTKLN program) will be scrapped completely due to numerous cases of alleged extortion.[33]

Brunei – Data protection Policy adopted

One previously unnoticed development is that the Brunei Government has adopted a *Data Protection Policy*[34] which has applied since at least early 2014 to government Ministries and Departments, including educational institutions and statutory bodies (with numerous and ill-defined exemptions). The exact legal status of the Policy is uncertain, but it contains no references to legislative authorisation, or even which specific government body made it. The Policy is not listed on the 'Policy' section of the Brunei government's e-government portal.[35] Its implementation is the responsibility of the E-government National Centre ('the Authority'), which administers the Brunei

---

[29] Data Privacy Act (Philippines), s. 42: 'Existing industries, businesses and offices affected by the implementation of this Act shall be given one (1) year transit ory period from the effectivity of the IRR or such other period as may be determined by the Commission, to comply with the requirements of this Act.'

[30] Staff author 'Toral: Appeal to President Aquino on Data Privacy Law' (*Sun Star, Cebu*, 16 December, 2014) <http://www.sunstar.com.ph/cebu/business/2014/12/16/toral-appeal-president-aquino-data-privacy-law-382356>

[31] 'Resolution directing the Committee on Information and Communications Technology to conduct an inquiry, in exercise of its power of oversight into the reported delay in the promulgation of the implementing rules and regulations of Republic Act no. 10173, otherwise known as the Data Privacy Act of 2012, as well as the delay in the formal establishment of the National Privacy Commission created under the Act' (HR01325); Status: Pending with the Committee on RULES since 2014-06-11; Item 49 at <http://www.congress.gov.ph/members/search.php?id=roman-r&pg=auth#>

[32] Fardah Pewarta 'Indonesia Interior Minister halts implementation of e-ID card project' (AntaraNews.com, 20 November 2014) <http://www.antaranews.com/en/news/96626/indonesia-interior-minister-halts-implementation-of-e-id-card-project>.

[33] Staff author 'Jokowi to Scrap ID Card for Indonesian Migrant Workers' (Jakarta Globe, 1 December 2014) <http://thejakartaglobe.beritasatu.com/news/jokowi-scrap-id-card-indonesian-migrant-workers/>

[34] Government of Brunei *Data Protection Policy*, undated, probably 2013

[35] See < http://www.gov.bn/en/SitePages/Policy.aspx> on the eDarussalam website.

government's IT systems., and there is provision for an Advisory Committee (no evidence of existence found). Breaches of the policy are to be investigated by the Authority and 'may be subject to Government disciplinary procedure', and prosecutions where relevant. The data privacy principles set out in the Policy are reasonably strong, going beyond the OECD minimum in various ways including collection minimisation, limiting data retention and restrictions on data exports. Under the policy, individuals are entitled to access and correction to their own records, and rights to complain of breaches to the agency concerned (which must inform the Administrator). The Administrator may investigate 'where necessary', but there is no stated right of appeal to the Administrator from agency decisions (or from the Administrator). A UK company has provided implementation training to Brunei officials. This initiative is invisible on the Internet, and evidence of its implementation is lacking.

This article is part of an update to Graham Greenleaf Asian Data Privacy Laws – Trade and Human Rights Perspectives *(OUP, 2014).*