Thailand's Draft Data Protection Bill: Many Strengths, Too Many Uncertainties

GRAHAM GREENLEAF AND ARTHIT SURIYAWONGKUL

(2018) 153 *Privacy Laws & Business International Report* 23
[2018] *UNSWLRS* 55

UNSW Law
UNSW Sydney NSW 2052 Australia

Thailand's draft data protection Bill: Many strengths, too many uncertainties

Graham Greenleaf and Arthit Suriyawongkul*

(2018) 153 *Privacy Laws & Business International Report*, 23-25

Thailand is the most economically significant country in East Asia which does not yet have anything resembling a general data privacy law (China and Indonesia have such laws with somewhat limited scope). That is likely to soon change, because on 22 May 2018, just before the EU's GDPR came into force, a draft *Personal Data Protection Bill* (PDPB) was approved by the Thai Cabinet for submission to the Council of State and the National Legislative Assembly, as previously promised by Pichet Durongkaveroj, the Minister of Digital Economy and Society (MDES).[1] Thailand has been ruled by a military junta (the National Council for Peace and Order) since the 2014 overthrow of the elected Yingluck Shinawatra government. Since the 2014 coup, Thailand has a unicameral National Legislative Assembly which is generally regarded as a rubber stamp for the government, so it is possible that developments will occur quickly after June.

After ten years of various draft Bills,[2] there are a number of reasons why the current Bill is much more likely to be enacted. A local factor is that lack of data privacy has recently become very controversial in Thailand because a mobile phone operator, True Move, exposed 46,000 customer records (names, addresses, scans of ID cards and passports) but apparently faces no legal consequences.[3] An external factor is the extra-territorial reach of the EU's *General Data Protection Regulation* (GDPR), in force as of 25 May 2018, which is referred to constantly (although often with exaggeration) by Thai commentators as posing problems for Thai businesses unless Thailand adopts a compatible law.[4]

The purpose of this article is to critically review the PDPB, by reference to the standards of international privacy instruments.

Scope, definitions and exceptions

The PDPB will apply to almost all of the private sector. It will not apply to uses of personal data for private purposes, or where data is collected specifically for media, artistic or literary uses, and collected according to professional ethics or for public benefit (s4(1)(2)). These are similar to internationally standard exceptions. Less usual is the complete exemption for credit information businesses, which already have more limited data privacy legislation.[5] It is

* An English language version of the full Bill is not yet available; Translation of some provisions are by Arthit Suriyawongkul and Nitchakarn Chantarapratin; other valuable assistance has been provided by Dhiraphol Suwanprateep, Nont Horayangura and Pattaraphan Paiboon (Baker & McKenzie), Clarisse Girot (ABLI), and David Duncan (Tilleke & Gibbons), All content is however the responsibility of the authors alone.

[1] Jirapan Boonnoon 'Legislation on way to boost data security', *The Nation*, 1 May 2018.

[2] G. Greenleaf *Asian Data Privacy Laws – Trade and Human Rights Perspectives* (OUP, 2014), Chapter 12, pp. 353-60.

[3] Suchit Leesa-Nguansuk 'New data law aimed at ensuring privacy' *Bangkok Post*, 1 May 2018 <https://www.bangkokpost.com/business/news/1455534/new-data-law-aimed-at-ensuring-privacy>

[4] For examples, see Thai researchers cited by Asina Pornwasin 'Govt in race against time to update data privacy law' *The Nation*, 7 May 2018 <http://www.nationmultimedia.com/detail/national/30344739>.

[5] Credit Information Business Act 2002 (in English) <https://www.imolin.org/doc/amlid/Thailand_Credit%20Information%20Business%20Act.pdf>. See updated definitions of "Information", "Information Processing", and "Credit Information Business" in 2008 amendment: <http://thailaws.com/law/t_laws/tlaw0068b.pdf >.

undesirable to exempt a whole sector rather than specific activities from general legislation like this. This is particularly so because this Bill provides that where there is an existing (sectoral) data protection law, provisions of this law are additional (s3(1)). The PDPB will therefore also strengthen Thailand's credit reporting privacy protections.

It appears that the PDPB applies generally to the public sector. The only relevant exceptions are of uses by legislative bodies or courts (s4(3)(4)) (which would be better if they specified the purposes exempted, not only the bodies). A public sector law giving very minimal privacy protection, the *Official Information Act 1997* (OIA) is two decades old and largely useless.[6] The PDPB will therefore apply to the public sector, supplementing and effectively supplanting the privacy aspects of the OIA (consistently with s3(1)). However, the OIA s22 has provision for Ministerial Regulations to exempt security agencies and other specified state agencies from its provisions where disclosure of personal information would obstruct their operations. How these provisions will interact with the PDPB's provisions (including exemptions by decree mentioned below) remains to be seen. Data privacy laws in most ASEAN countries have little or no applicability to the public sector, including in Singapore, Malaysia, Vietnam and (as yet) Indonesia.

The definition of 'personal information' (s6) is conventional, based on identifiability. There is a 'business contact' exception for 'an identification of only name, position, working place, or business address', which may be too broad because business-related information (e.g. email address) is often provided for personal purposes only. Singapore's definition of 'business contact information' is preferable because it requires that the specified types of information are 'not provided by the individual solely for his personal purposes'.

There is no definition of 'data processing'. The PDPB use a group of words 'collect, use, and disclosure' repetitively in places (which is more common in jurisdictions influenced by the OECD Guidelines). The word 'collect' in Thai can have various meanings, including 'gathering', 'filing', and (in some opinions) 'retaining', and the PDPB is unclear which meaning is intended. This could be problematic in disputes.

Exemptions from the scope of the Act may also be made by Royal Decree (s4), a power with no defined limitations or criteria for exercise. There is further scope for exceptions by Ministerial Regulations, without legislative limits or criteria, in relation to collection of personal data (ss21, 22, 23) and use and disclosure of personal data (ss24, 25). This unlimited executive power to exempt mars the PDPB, and may cause difficulties with international standards.

Extra-territorial application

The PDPB applies to collection use and disclosure of personal data which occurs in Thailand, no matter where controller or processor is located (s5). Wide extra-territorial application may result.[7]

[6] Greenleaf, 2014, 356-8

[7] Baker & McKenzie put it 'Data controllers and data processors who collect, use, or disclose personal data outside Thailand but (1) any parts of such actions occurred in Thailand; or (2) the consequence of such actions intentionally to be occurred in Thailand; or (3) the consequence of such action should occur or it could be foreseen that the consequence would occur in Thailand, are subject to the Amended PDPB.' 'New Draft Thai Personal Data Protection Bill - Extraterritorial Applicability Introduced' *Baker & McKenzie Client Alert* 18 April 2018.

A complex data protection authority (DPA) lacking independence

The administrative structure set out in the PDPB is complex, comparable only to that in Korea (and was anticipated in earlier Bills), with responsibility distributed among the following.

- ***The Personal Data Protection Committee (PDPC)*** – The PDPC has 15 members plus a Secretary-General, drawn from government, business, and the professions (ss8-16). There is no legislative requirement on the Committee or its members to act independently, and it has no other guarantees of independence. A requirement on members to 'leave the room if there can be conflict' (s13), is a very weak safeguard. The PDPC has very broad functions (s14) that include making guidelines; making compliance orders (s14(4)); making codes of conduct; determining criteria of sufficiency for data exports (s14(5)); determining administrative fines and submitting enforcement cases to the Administrative Court (s14(7)); recommending law reform related to personal data protection (s14(8)); recommending regulations to be made by the Cabinet (s14(9)); and interpreting issues in relation to law enforcement (s14(11)).

- ***The Office of the Personal Data Protection Committee (OPDPC)*** (ss32-56) – OPDPC is a statutory corporation (s32) with an unspecified number of members. It performs research and administrative tasks for the PDPC, OPDPC Oversight Committee, Expert Panels, and subcommittees (s33). The Minister has sweeping powers to 'supervise in general the affairs' and 'to suspend actions' of the OPDPC, including to ensure that its operations are consistent with Cabinet resolutions (s56),[8] so it has no formal independence. While Thai legislators may claim that these Ministerial powers are normal, they will negate the Office being considered as independent from an EU (or ICDPPC) perspective.

- ***The Secretary-General of the OPDPC (SG-OPDPC)*** (ss43-53) – The SG-OPDPC is the closest role to a 'Data Protection Commissioner', but has no independence from the OPDPC, and the OPDPC is not independent of the Minister. The Secretary-General is appointed by the OPDPC (s43), and is limited to two four-year terms (s45). His or her powers do not seem to be independent of the OPDPC (ss48-51).

- ***The Oversight Committee of the OPDPC*** (s36) – As if all of the above was not enough layers of bureaucracy, a ten-person committee (including the Secretary-General OPDPC), appointed by the Minister or ex-officio, oversights the Office.[9]

- ***Panels of experts for mediating complaints (Panels)*** (ss57-62) – Complaint resolution is by Panels of experts (there may be multiple Panels) appointed by the PDPC (s57), with duties are to consider complaints, investigate and 'mediate' (s58), under regulations made by the PDPC (s59). Panels may issue orders prohibiting or requiring actions by controllers (s60), can trigger administrative enforcement (including fines) if controllers do not comply with orders (s60). Their role is more like

[8] 'Minister shall have general oversight power over the operation of the Office, to ensure its operations go according to its related legal power and duties, government policy, strategic plan, and cabinet resolution. Minister shall has power to order the Secretary-General for fact reporting, comments, and representation, and has power to suspend actions of the Office that contradict related the power and duties of the Office, government policy, strategic plan, or cabinet resolution. Minister can also order for interrogation on the operations of the Office.' (s56 – unofficial translation of part only).

[9] Chairperson appointed by the Minister; Permanent Secretary of the Ministry of Digital Economy and Society; Secretary-General of the National Digital Economy and Society Committee; six qualified members appointed by the Minister; and Secretary-General OPDPC.

arbitration, not mediation, because Panels issue enforceable orders. Panels with a similar role are established under Korean law.[10]

Data protection principles

The PDPB's data protection principles, whether expressed as obligations of data controller or rights of data subjects, include many elements which reflect those in EU law (whether the 1995 Directive or the 2016 GDPR), and these are marked **in bold** in the following discussion. However, many of these obligations and rights can be changed by Ministerial Regulations.

Collection of personal data requires the consent of the data subject before or at time of collection, must be written, and **consent may be withdrawn** at any time (s17). Notice must be given to the data subject about specified matters at time of collection (s20). Collection must generally be **from the data subject** (s22). There is a general exception for when another law provides otherwise (so the PDPB is inferior to other laws) (s17), and specific exceptions for collection **without consent** (s21), including for public interest or 'legitimate interests of the controller' (with a **test of balancing** against the fundamental rights and freedoms of the data subject, as in the GDPR); or as authorised by law, or as prescribed in Ministerial Regulations. Data collection can be 'only carried out to the extent that it is necessary within a lawful purpose of the personal data controller' (s19), which implies **minimal collection** only.

The data subject's informed **consent is required prior to any secondary use or disclosure,** unless it is authorised by the PDPB or another law (s18).

In relation to **sensitive data** the PDPB prohibits collection of personal data concerning 'ethnicity; race; political opinions; doctrinal, religious or philosophical beliefs; sexual behaviour; criminal records; health information, or any other information that affects the public's feelings as prescribed by the Committee' (s23) unless it is 'for the protection of or harm prevention to life, body, or health of a person' (s21(2)) or 'for legal compliance or the use of state power by the data controller' (s21(7)). Other categories prescribed in Ministerial Regulations of course can be additionally exempted from the prohibition. There is no additional protection of genetic or biometric information as the GDPR requires.

Controllers have obligations to undertake **personal data impact assessments** 'on a regular basis' (s29(1)). Data controllers must provide appropriate security measures (s29(2)), including ensuring that others to whom personal data is provided (processors) have security measures (s29(3)). **Data breach notifications** must be given to the data subject 'without delay' with no specific deadline, and also to the PDPC if a breach exceeds a magnitude to be specified by the PDPC (s29(5)). A report of 'the result of the remedial measure' to the PDPC also only needs to be made if the specified magnitude is exceeded. Unlike some data privacy laws, it is the obligation to notify the data subject that is absolute.

Processors have direct obligations to act only on the controller's instructions, to provide the required level of security, and to inform controller of data breaches (s30). They thus have exposure to enforcement and compensations actions.

Data subjects have normal rights of access, subject to exceptions provided (s26), and the right to seek corrections or have personal data brought up-to-date (s28).

Data controllers must destroy personal data automatically on the **expiry of the retention period** determined by the purpose of collection (s29(4)). In addition, where it is claimed that

[10] See Greenleaf *Asian Data Privacy Laws*, pp. 150-151 concerning Personal Information Dispute Mediation Committees.

a controller is in breach of the Act, data subjects have the right to request deletion or **temporary suspension of processing** or de-identification (s27), and to complain to a Panel if refused. PDPC can determine the criteria to be followed.

Data export limitations

Transfer of personal data to foreign countries must meet a standard of privacy protection set by the PDPC under s14(5), but otherwise not prescribed by the Act. The PDPC could set 'the same standards as this Act', or higher or lower standards. The usual exceptions are allowed (consent, necessary for contract etc). These provisions, in the absence of PDPC standards being set, are almost certainly too vague to satisfy EU concepts of adequacy.

Data exports are also allowed in 'other cases as prescribed in the Ministerial Regulations' (s25(5)). This would allow the possibility of foreign companies certified under APEC CBPRs being allowed to receive data exports from Thailand, simply because of their APEC-CBPRs compliance. However, Thailand has not indicated any intention to join APEC CBPRs. The related concept of certification marks (and recognition of foreign certification marks) as a basis for data transfers has been removed from this version of the PDPB.[11]

Remedies for breaches

A court or the PDPC (the provision is not precise) is empowered to **award compensation** for damage (s64). To avoid liability for damages, a controller has the onus to establish it was 'fully compliant' with legal requirements (including guidelines made by the PDPC), or acting on order of officials, or subject to *force majeure*.

Administrative fines up to 500,000 baht (US$16,000) may be levied by the PDPC, in relation to breaches of specific sections of the PDPB (ss69-74, s14(7)). PDPC may take administrative fines before the Administrative Court to enforce them (s75). These maximum fines are derisorily small compared with the fines now possible under most other new laws, and relative to size of e-commerce.

Various criminal offences, with possible prison sentences, apply to breaches of specific sections of the PDPB (ss65-66). Prison sentences have been re-introduced after removal from earlier versions of the PDPB. The PDPC also has a role in settling or compounding fines where a person is charged with a criminal offence (s68). The PDPC can compound criminal offences, accepting a payment of a fine instead (s68). There is no mention of how to appeal against a criminal sentence.

Timing and transitional arrangements

The Act will come into force one year after publication in the Government Gazette. Previously collected data is subject to an opt-out provision (s83), rather than requiring positive consent to be obtained, and no notice is required to the data subject ('owner') for continuing use. This opt-out replaces a three-year grace period to obtain consent for use of previously collected data.[12]

---

[11] Baker & McKenzie 'New Draft Thai Personal Data Protection Bill - Extraterritorial Applicability Introduced' *Baker & McKenzie Client Alert* 18 April 2018.

[12] 'The Amended PDPB removes the 3-year grace period for collection of retrospective consent to the use of the personal data collected before the enactment of the PDPB and uses an opt-out mechanism instead. Under this Amended PDPB, data controllers can use previously collected data and continue to use such data in accordance with the original purposes. However, the data controller must provide and publicize a procedure to allow the data subjects to easily revoke their consent. For the disclosure of the data or the conducting of any other activity related thereto, the data controller is required to comply

Conclusions

The most recent (April 2018) version of Thailand's *Personal Data Protection Bill* is both comprehensive of the basic elements of a data privacy law, and with many additional aspects that reflect the 'European' elements of the Directive and the GDPR, compatibility with which appears to be an objective of the Thai government. These strong elements are noted in bold in the previous discussion, and need not be repeated. There is no question that for businesses operating in Thailand, this Bill imposes serious obligations, and for data subjects it creates serious rights and remedies not previously available.

However, there are aspects of the Bill that undermine its objective to provide credible data privacy protection. Thai NGOs have published criticisms.[13] Its complex administrative and enforcement structure raises difficulties in determining who could be held responsible for effective enforcement. However, the main problem is its absence at any level of independence from governmental and Ministerial control. The Bill is also riddled with the potential for excessive exemptions and exceptions to be made both by Royal Decree and by Ministerial Regulation (which may or may not occur).

The lack of a right of appeal against decisions of the PDPC or of expert Panels is a surprising omission. Appeals against administrative decisions (such as by the PDPC) in Thailand can be made to the Administrative Court and further to Supreme Administrative Court. However, where this is not explicitly stated, there are more likely to be procedural delays, so an explicit appeal right would be preferable. Other matters now commonplace in data privacy laws of the 126 countries that have them are standards for foreign transfers that are set by the Act, not by the DPA; explicit opt-out provision for direct marketing; and administrative fines that are more than trivial.

In relation to alignment with the GDPR, it should also be noted that there are many elements that are missing, even though they are also absent from most of the world's current privacy laws outside the EU. These include: inclusion of genetic and biometric data as sensitive data; requirements to appoint data protection officers (DPOs); limits on decisions made through automated processing; privacy by design and by default; data portability; and a right to de-linking (right to be forgotten).

Thailand's Bill is one of reasonable strength by current global standards, except for its major deficiencies in the independence of its DPA, and the excessive degree of potential exceptions to its operation.

Authors: *Graham Greenleaf, Asia-Pacific Editor, is Professor of Law & Information Systems at UNSW Australia. Arthit Suriyawongkul a Board Member and Secretary of the Foundation for Internet and Civic Culture, Thailand and Guest Lecturer, Faculty of Sociology and Anthropology, Thammasat University, Bangkok.*

with the Amended PDPB'. 'New Draft Thai Personal Data Protection Bill - Extraterritorial Applicability Introduced' *Baker & McKenzie Client Alert* 18 April 2018.

[13] Asina Pornwasin 'Thai data protection falls short of EU benchmark' Open Development Thailand, 26 May 2018 <https://thailand.opendevelopmentmekong.net/news/thai-data-protection-falls-short-of-eu-benchmark/>.