Thailand – Asia's strong new data protection law

Graham Greenleaf and Arthit Suriyawongkul
[2019] 160 *Privacy Laws and Business International Report* 1, 3-6

A military coup in 2014 imposed a *junta* government in Thailand. In February 2019, three weeks before the first general elections since the coup, this government enacted a data privacy law to override an old and ineffective law applying only to the public sector. A military-backed party now leads a coalition government with a Prime Minister and Cabinet members from the previous military government, and an appointed upper house.

Most of the *Personal Data Protection Act* (PDPA)[1] does not come into force until 28 May 2020, a year after it was gazetted, but some provisions concerning the data protection authority are in force during this interim period. The PDPA is based on a GDPR-influenced Bill proposed in May 2018,[2] but it has many differences from that Bill. The Act establishes a Personal Data Protection Committee (PDPC) and an Office to act on its behalf.

Scope and exemptions

The PDPA is a comprehensive Act, in that it covers both the private and public sectors. Of ASEAN countries, only the data privacy law of the Philippines also covers the public sector.

The PDPA exempts few parts of the private sector, but further exemptions can be made by decree. It will not apply to uses of personal data for private and household/family purposes (depending on translation), or where data is collected specifically for media, artistic or literary uses, and collected according to professional ethics or for public interest (ss. 4(1) and (3)). Less usual is the complete exemption for credit bureaus and their members (s. 4(6)), which already have more limited data privacy legislation.[3] It is 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,[4] provisions of this law are additional (s. 3). The PDPA would therefore strengthen Thailand's credit reporting privacy protections, if it was not entirely exempted.

The public sector exemptions are limited: for state agencies with duties to protect public security, including financial security of the state or public safety, including preventing money laundering, forensic science, or cybersecurity (s. 4(2)). Also exempted are parliamentary matters and the operation of the courts (ss. 4(4) and (5)). These are broadly similar to internationally standard exceptions, but tend to exempt the 'operations of' a type of entity, rather than to exempt by reference to specific purposes of processing (as the EU's GDPR

---

[1] *Personal Data Protection Act 2019 (unofficial English translation)* <http://www.mdes.go.th/assets/portals/1/files/The%20Personal%20Data%20Protection%20Act%20-%2019-6-19.pdf >.

[2] The 2018 Bill is examined in G. Greenleaf and A. Suriyawongkul 'Thailand's draft data protection Bill: Many strengths, too many uncertainties' (2018) 153 *Privacy Laws & Business International Report*, 23-2

[3] Credit Information Business Act 2002 (unofficial English translation, last amended in 2016) <https://www.ncb.co.th/about-us/credit-infomation-business-act>. See Section 3 for the definition of "Financial Institution" which includes commercial bank, credit card company, and insurance company, among others. This financial institution list can be amended by Credit Information Protection Committee, which together with PDPA s. 4(6) means the Credit Information Protection Committee also has a power to grant PDPA exemptions to a type of business.

[4] There are at least eight such laws, covering credit bureau, telecommunications, health information, banks and finance companies, securities companies, and electronic payments; David Duncan 'Jurisdiction Report: Kingdom of Thailand' in Girot, C. (Ed.) *Regulation of Cross-border Transfers of Personal Data in Asia*, Asian Business Law Institute, 2018.

does). Subject to those exceptions, the PDPA appears to apply generally to the public sector. However, a public sector law giving very minimal privacy protection, the *Official Information Act 1997* (OIA) is two decades old and largely useless.[5] The PDPA will therefore apply to the public sector, supplementing and effectively supplanting the privacy aspects of the OIA (consistently with s.3(1)), allowing complaints against the public sector to be made under the PDPA. However, the OIA s.22 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 PDPA's provisions (including exemptions by decree mentioned below) remains to be seen.

Exemptions from the scope of the Act may also be additionally made by Royal Decree (s.4), a power with virtually no defined limitations or criteria for exercise, apart from a generic 'for public interest' clause. However, similar powers in the Bill to exempt by Ministerial Regulations have been removed. The data controllers under exemptions specified in ss. 4(1)-(6), or by Royal Decree, must nevertheless provide 'a security protection of personal data in accordance with the standard' (s. 4), which refers to the security standard to be prescribed under s. 37(1)), so it is not a complete exemption. However, none of these exemptions (including that for media, artistic or literary uses) are moderated by a necessity and/or proportionality test, as is best practice. Royal Decrees are announced by the Minister, but can be on the advice of the PDPC (s. 16).

The PDPA will have extra-territorial effect (similar to the GDPR) in relation to marketing to, or monitoring of, persons in Thailand. Processing outside Thailand by a controller or processor located in Thailand is also covered (s.5).

The definition of 'personal information' is conventional, based on identifiability ('enables … identification …whether directly or indirectly': s. 6) . It does not explicitly include the linkage to data to which the data controller has or is likely to have access, unlike, for example, in Singapore[6]. There is no exception for publicly available information or (unlike the Bill), 'business contacts'. There is no definition of 'data processing', nor a defined list of lawful reasons for processing, which is a significant difference from the GDPR. The PDPA use a group of words 'collect, use, and disclosure' repetitively in places. The word 'collect' in Thai can have various meanings, including 'gathering', 'filing', and (in some opinions) 'retaining', and the PDPA is unclear which meaning is intended. This could be problematic in disputes.

Many GDPR-informed principles, some omissions

Many of the PDPA's stronger principles are informed and influenced by the GDPR, although not copied from it. These include: data minimization in collection (s. 22); strong consent requirements in relation to collection (ss. 23-25) perform a similar function to GDPR 'legitimate processing' restrictions; the right to data portability, subject to many limitations (s. 31); the right to object to processing (s. 32); right to request deletion, in terms similar to the GDPR and including the 'right to be forgotten' (s. 33); genetic and biometric data have been added to the categories of 'sensitive' personal data that has more restrictive processing conditions (s. 26), consistent with the GDPR and unlike the previous Bill.

Appointment of data protection officers (DPOs), called 'personal data officers', is required (s. 41), with exceptions for those state agencies specified by the PDPC, and 'small sized

[5] Greenleaf, *Asian Data Privacy Laws* (OUP, 2014), 356-8

[6] Singapore's definition of 'personal data' is "data,… about an individual who can be identified — (a) from that data; or *(b) from that data and other information to which the organisation has or is likely to have access;*" - *Personal Data Protection Act 2012* (Singapore) <https://sso.agc.gov.sg/Act/PDPA2012>.

businesses' which have a 'large amount' of personal data (criteria to be specified by PDPC), and are not in the business of processing sensitive data). These DPO requirements were not found in the previous Bill. A group of enterprises may designate a joint DPO under some circumstances (s. 41). DPOs are given some protections against dismissal for performing their duties and must be able to report directly to senior management (s. 42).

A data processor bound by the PDPA but located outside Thailand must designate an in-country representative who has power to act in relation to all matters concerning personal data, and liability for failure to do so (s. 37(5)).

Security must be both 'appropriate' and meet minimum standards set by the PDPC (s. 37(1)), with recipients of personal data required to adhere to the same standard. Notification of data breaches to the PDPC Office is required within 72 hours, unless the breach does not raise any risks, and to the data subject if a breach raises high risks (s. 37(3)).

Processors have direct obligations to act only on the controller's instructions, to provide the required level of security, to inform the controller of data breaches, and to maintain records of processing (with exceptions for most small businesses) (s. 40). They thus have exposure to enforcement and compensations actions.

Thailand has chosen not to include in the PDPA some notable aspects of the GDPR, such as privacy by design and by default, and protections in relation to automated processing, are not included in the PDPA. There is no obligation on controllers equivalent to the GDPR's 'demonstrable accountability', only a list of items that must be maintained for the data subject and the PDPC Office to check (s. 39). Unlike the previous Bill, controllers do not have obligations to undertake 'personal data impact assessments' in some circumstances.

PDPC and its Office – Permanent and interim arrangements

A Personal Data Protection Committee (PDPC) is established as the primary body to administer the law, but it has no legislatively nor financially guaranteed independence. Chapters 1 and 4 of the PDPA, establishing the PDPC and the Office of the PDPC, are already in force, as are Transitional Provisions (ss. 91-96, but not ss. 94-95), setting out their interim operations during the year before the Act comes fully into force ('transitional period'). The functions of Secretary of the Office will be carried out by the Deputy Permanent Secretary of the Ministry of Digital Economy and Society, but the Office must be formally established before the transitional period concludes (s. 93).

The administrative structure established by the PDPA is complex:

- ***The Personal Data Protection Committee (PDPC)*** – The PDPC has 17 directors, drawn from government, business, and the professions (ss8-14). 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 not to attend meetings discussing matters in which they have a direct or indirect interest, and to inform the PDPC of such matters (s. 15), is a very weak safeguard. The PDPC will initially consist of six ex-officio members who are all very senior civil servants (ss. 8(2) and (3)). Within 90 days of the Act coming initially into force (ie by 27 August 2019) the Office should have finalized the appointment[7] of the Chairperson of the PDPC (s.8(1)) and nine 'honorary directors' (s.8(4)), all of whom must have qualifications relevant to

[7] They must be appointed by a Selection Committee (s.9), complying with disqualifying criteria (s. 10), for a term of four years, with re-appointment for 'not more than two terms'.

privacy. (s.12), but this is still being completed. The Secretary-General of the PDPC's Office is also a director.

- ***The Office of the Personal Data Protection Committee (OPDPC)*** (ss32-56) – The Office of the PDPC is a government agency (s. 43), but is a legal entity (like a statutory corporation), rather than being classed as part of the administrative structure. It has the duty to perform technical and administrative tasks for the PDPC, with a long list of specific powers and duties (s. 44). These include 'to follow up on and evaluate compliance with' the Act (s. 44(10)). It performs tasks not only for the PDPC, but also for the OPDPC Oversight Committee, Expert Panels, and subcommittees (ss. 44 and 45(6)). Unlike in the previous Bill, the Minister no longer has specific sweeping powers to control the activities of the OPDPC.[8] Although the Office can seek funding from various sources, including subsidies from international governmental organizations and fees from the Office's operations (s. 46), essentially the Office and the Committees are financial dependent to 'general grants as reasonably provided by the government on a yearly basis'. The Office cannot have its own reserves to guarantee the adequate resource in the event of budget cut, as all the funds and properties of the Office 'are required to be submitted to the Ministry of Finance as public revenue' at the end of fiscal year.

- ***The Commission Supervising the Office of the PDPC*** (ss. 48-56) – As if all of the above was not enough layers of bureaucracy, a ten-person committee (including the Secretary-General OPDPC), selected by another eight person selection committees, oversights the Office.[9]

- ***The Secretary-General of the Office of the PDPC (SG-OPDPC)*** (ss. 57-65) – The SG-OPDPC is in charge of administering the Office of the PDPC, is appointed by the Commission supervising the OPDPC (s. 57), and reports to it (s. 63). The SG can be appointed for two four-year terms. The SG is a Director of the PDPC, but has no independent powers and is not equivalent to a 'Data Protection Commissioner'.

- ***Expert Committees for arbitrating complaints*** (ss. 71-76) – Complaint resolution is by Expert Committees (one or more) appointed by the PDPC (s. 71). Their duties are to consider complaints, investigate and 'resolve disputes' concerning personal data (s. 72), under regulations made by the PDPC (s. 73). Expert Committees may issue orders prohibiting or requiring actions by controllers (s. 74), and can trigger administrative enforcement (including fines) if controllers do not comply with orders (s. 74), in accordance with Thai administrative law. This is arbitration, not mediation, but otherwise has some similarities to mediation committees established under Korean law.[10]

Overall, this a very diffuse structure for a data protection authority, with the PDPC, its Chairperson, its Secretary-General, and its Expert Committees all playing somewhat separate and independent roles. However, it is the PDPC as a whole which is of greatest importance.

---

[8] See s. 56 of the previous Bill, discussed in Greenleaf and Suriyawongkul above.

[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.

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

The PDPC has very broad functions (s. 14) that include: establishing a 'masterplan' for data protection; making guidelines for compliance; making compliance orders; making codes of conduct; establishing guiding principles for data exports; recommending law reform (including a five-yearly review of the Act); recommending regulations to be made; and advising on the interpretation of the Act. The PDPC's power under the previous Bill to determine administrative fines and submit enforcement cases to the Administrative Court is no longer listed.

Notifications and Regulations must be made by the Minister during the transitional period (s. 96). The Minister of Digital Economy and Society (MDES) is responsible for the Act (s. 7).

Once the PDPC is fully in force, data controllers my continue to use personal data for the original purpose of collection, but must establish a procedure for data subjects to opt out of such continuing use (s. 95).

PDPC – A DPA with multiple means of enforcement

The PDPA provides for civil, criminal and administrative liability, providing a good basis for a system of responsive regulation.

The starting point is that the PDPC's Expert Committees can order compliance by controllers or processors. Many breaches of the PDPA can result in administrative fines, with maximum fines ranging from 500,000 baht (approx. US$ 16,000) to 5 million baht (approx. US$160,000) (ss. 82-89), depending on nature of the breach. These are now a low maxima by international standards, but may still be a deterrent to some local businesses. The highest is however a ten-fold increase on the maximum of 500,000 baht in the previous Bill. These administrative fines are levied by the Expert Committees, and if they are unpaid the Expert Committees can file a case in the Administrative Court of First Instance to enforce them (s. 90). In effect, this provides a right of appeal, and it is likely that the Court will require all the evidence to be submitted to it, and (in effect) re-hear the question of the substantive breach, not only the question of quantum of damages. Appeals against administrative decisions in Thailand can be made to the Administrative Court of First Instance and further to the Supreme Administrative Court.[11]

Data subjects have a right to seek compensation from a court (not from the PDPC) for any breaches of the Act, without need to prove intent or negligence. The onus is on the controller or processor to prove that the damage is a result of *force majeure* circumstances or the data subject's actions or inaction, or that they were acting on order of officials, (s. 77). The court may impose additional compensation up to double the original amount (i.e. 'triple damages') (s. 78). Data subjects are therefore not reliant upon the PDPC's Expert Committees in order to obtain remedies.

Various criminal offences, with possible prison sentences, apply to breaches of specific sections of the PDPA (ss. 79-81), including for disclosures to third parties following authorised access to personal data. No right of appeal is specified, but appeals would normally go to the Court of Appeal. Prison sentences have been re-introduced after removal from earlier versions of the Bill.

Data exports and localisation

Data exports from Thailand can occur to countries which provide an 'adequate level of protection' (s. 28). However, 'adequate' is to be determined by criteria set by the PDPC, so it

[11] See s. 42, *Act on Establishment of Administrative Courts and Administrative Court Procedure*, B.E. 2542 (1999) <http://www.admincourt.go.th/admincourt/upload/webcmsen/The%20Institution/The_Institution_100118_145007.pdf>.

cannot be assumed that it will mean the same as it does in the EU, requiring protections that are 'essentially equivalent' to the protections under the PDPA. The previous Bill also allowed data exports as prescribed by Ministerial Regulations, but that has now been dropped.

Data exports are allowed under reasonably standard provisions concerning requirements of other laws, contractual clauses in the interests of the data subject, reducing harms where consent is not possible, and protection of public interests (s. 28). Data subject consent is a sufficient basis for exports, provided only the data subject is informed that there is no adequate level of protection in the destination country, which is far too weak a safeguard to ensure sufficiently informed decisions. Additional provisions allowing data exports include a form of Binding Corporate Rules (BCRs), and other undefined 'suitable protection measures which enable the enforcement of the data subject's rights, including effective legal remedial measures', both to be based on standards set by PDPC (s. 29). These 'appropriate safeguards' (in GDPR terminology) might include standard contractual clauses or a certification mechanism.

However, mere certification of a foreign company as compliant with the APEC-CBPRs scheme should not be considered by PDPC to satisfy these criteria, both because the data protection standards required by APEC-CBPRs fall so far below those of the PDPA, and also because a breach of APEC-CBPRs does not in itself result in any 'legal remedial measures' (effective or otherwise), but only loss of accreditation (which has never happened). The European Commission, in its adequacy decision concerning Japan, has made it clear that an 'onward transfer' of EU-origin personal information cannot be based on APEC-CBPRs certification.

Data localization (both local copy requirements, and export prohibitions), which are significant in Vietnam and Indonesia, and promised in India, have had no effect on Thai law as yet. The Thai *Cyber Security Act* was also enacted in February 2019, but does not include explicit data localisation provisions, although some of its provisions could be applied to personal data.

Conclusions: A potentially very significant law

The main significance of the Thai law is that it is the first explicitly 'GDPR-based' law to yet be enacted in Asia. While there are GDPR-informed draft Bills in India and Indonesia, they have not yet reached the stage of being introduced in their legislatures. Korea's laws already anticipate many aspects of the GDPR (but have some significant weaknesses), and Japan's laws remain largely uninfluenced by it (despite the adequacy finding in its favour). While not all of the innovations of the GDPR's data protection principles are included in the PDPA, a substantial set are included, and they are more extensive than in the previous Bill.

Following the 2019 elections, the EU is again willing to re-commence negotiations on a free trade agreement (FTA) with Thailand and is its third-largest trading partner. Singapore and Vietnam both completed FTA negotiations with the EU in 2019, and progress with Thailand is the logical next step in the ASEAN region.[12] Parallel discussions between the parties on a possible adequacy finding or alternative data export measures, under the GDPR, might then take place.

For businesses operating in Thailand, this Act imposes serious obligations, but to assess their full extent they will need to obtain much further information which is not yet available, such as: the exemptions by Royal Decree; the s. 37(1) security standards; the s. 37(4) rules for notification of data breaches; the s. 38 criteria for 'small sized businesses'; 'appropriate

[12] William Hicks 'EU ambassador upbeat on Thai FTA talks' *Bangkok Post*, 9 September 2019 <https://www.bangkokpost.com/business/1746294/eu-ambassador-upbeat-on-thai-fta-talks>.

safeguards' allowing exports (s. 29); and the s. 41(2) requirements for appointment of a Data Protection Officer. There is much more which the PDPC also has to determine. Although s.96 says that such 'regulations and notifications' must be issued within a year of the Act coming into effect (ie by May 2020), s. 2 in effect contradicts this by delaying s. 96 coming into effect until May 2020. However, s, 96 also provides that 'If such cannot be carried out, the Minister shall report to the Cabinet the reasons thereof', so it may be that is the only sanction applicable. More clarity is needed on this.

For data subjects the PDPA creates serious rights and remedies not previously available, and the Act overall is a major step forward. From the perspective of Civil Society, the complex administrative and enforcement structure of the Act raises difficulties in determining who could be held responsible for effective enforcement, there is still no clear independence of the PDPC or its Office from government and Ministerial control. The potential scope of exemptions for security agencies, financial institutions, and control of money laundering, and for those made by Royal Decree are also of great concern.

The enforcement mechanisms in the Act are all much stronger than in the previous Bill. Rights of appeal against administrative fines and other decisions of the PDPC or its expert Committees, and in criminal prosecutions, might benefit from some further clarity.

Considered overall, Thailand's *Personal Data Protection Act* is much stronger than the previous Bill, both in terms of its principles and its enforcement. However, the picture will not be complete until the many rules that can be made by PDPC, and any Royal Decrees granting exemptions, are made. If the PDPA is well-administered it may become one of the strongest data privacy laws in Asia.

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.* *Very valuable comments and information have been received by the authors from Clarisse Girot, Director of the Privacy Project of the Asian Business Law Institute (ABLI), and from other correspondents in Thailand and elsewhere who prefer to be unnamed,, however responsibility for all content remains with the authors.*