

PDPA for Foreign Businesses in Thailand: What You Must Know

By Eksiam Chaisorn, Legal Consultant
Eksiam & Partners Co., Ltd.

This article is general legal information, not a legal opinion on any specific matter. Each matter must be assessed on its own facts and evidence. The latest online version is at <https://eksiamlegal.com/articles/pdpa-foreign-business.html>

Key points

- Key points
- I. Introduction: Why Foreign Businesses Cannot Ignore Thailand's PDPA
- II. Who Is Subject to the PDPA? (Territorial Scope)
- III. Data Controllers vs. Data Processors
- IV. Six Lawful Bases for Processing Personal Data
- V. Sensitive Personal Data: The Stricter Category
- VI. Eight Rights of Data Subjects
- VII. Cross-Border Data Transfers
- VIII. Thailand's PDPA vs. the EU's GDPR: Key Differences



- IX. Penalties
- X. Practical Checklist for Foreign Businesses
- **The Act follows the data subject, not the company.** Section 5, paragraph two applies the PDPA to a controller or processor outside Thailand that offers goods or services to people in Thailand or monitors behaviour taking place here.
- **Consent is the rule; Section 24 is the exception.** Section 19 bars collection, use or disclosure without consent, and Section 24 lists the six grounds, archiving and research, vital interests, contract, public task, legitimate interests, legal obligation, that displace it.
- **The sensitive-data list in Section 26 is open, not closed.** It requires explicit consent and ends with a catch-all for any other data the Committee prescribes as affecting the data subject in the same manner.
- **Access requests run on a thirty-day clock.** Sections 30 to 36 grant access, portability, objection, erasure, restriction and correction; Section 30 paragraph four requires an access request that cannot lawfully be refused to be met within thirty days of receipt.
- **There is no Thai adequacy list to rely on.** Section 28 measures the destination against rules the Committee prescribes under Section 16(5) and otherwise allows six exceptions; transfers inside one group run on a policy under Section 29.
- **Administrative fines are tiered at one, three and five million baht.** Sections 82, 83 and 84 set the three ceilings, the highest reserved for sensitive data, and Section 79 adds imprisonment of up to one year where sensitive data is misused for unlawful gain.

Thailand's Personal Data Protection Act binds a company on the strength of where the data subject is, not where the company is registered. This article sets out who Section 5 catches, what Sections 19 and 24 require before data may be processed, the rights granted by Sections 30 to 36, the transfer rules in Sections 28 and 29, and the penalty tiers in Sections 79 and 82 to 84.



I. Introduction: Why Foreign Businesses Cannot Ignore Thailand's PDPA

Thailand's PDPA binds any organisation that handles the personal data of people in Thailand, wherever that organisation sits. Section 5, paragraph two extends the Act beyond Thai borders, so a company with no office, staff or bank account in the kingdom can still owe the full set of duties and face administrative fines under Sections 82 to 84.

If your company collects, uses, or stores personal data from Thailand, whether from employees, customers, or website visitors, you are likely subject to Thailand's Personal Data Protection Act.¹ This is true even if your business is registered overseas and has no physical presence in the kingdom. The PDPA has *extraterritorial reach*, meaning it catches any organization that processes personal data of people in Thailand, regardless of where the company itself is based.

For foreign businesses, this creates a legal obligation that extends far beyond Thailand's borders. Unlike some privacy regimes that only apply to domestic enterprises, the PDPA holds foreign companies to the same standard as Thai-registered companies. Failure to comply can result in administrative fines of up to 1, 3 or 5 million baht depending on which duty is breached (Sections 82-84), criminal penalties including imprisonment, and civil liability for damages.

This article is a practical guide for international companies navigating the PDPA. We examine who must comply, the key obligations, the rights of data subjects, and how Thailand's approach compares to other leading privacy regimes like the European Union's GDPR.

II. Who Is Subject to the PDPA? (Territorial Scope)

Section 5, paragraph two catches a foreign controller or processor on either of two limbs: offering goods or services to data subjects in Thailand, whether or not they pay, or monitoring behaviour that takes place in Thailand. The second limb covers analytics, tracking cookies and profiling, so a site that sells nothing here may still be caught.

The PDPA's extraterritorial reach is set out in Section 5, paragraph two.² The Act applies to any *data controller or data processor* who is located outside Thailand, provided that:



(a) The organization offers goods or services to data subjects in Thailand; or (b) The organization monitors the behaviour of data subjects in Thailand.

This language is similar to Article 3 of the EU's General Data Protection Regulation (GDPR), which extends to "any organisation worldwide" that offers goods or services or monitors behaviour of EU residents. The practical effect is the same: if you run an e-commerce site, mobile app, or online service accessible to Thai users, you are processing personal data of Thai residents and the PDPA applies.

The second limb, "monitoring behaviour", captures activities like using analytics, tracking cookies, and profiling. This means that even if you do not sell anything in Thailand, if you collect behavioural data from Thai visitors to your website, you must comply with the PDPA.

Key Point: Extraterritorial Reach

The PDPA applies to foreign companies if they: (a) offer goods or services to Thai residents, or (b) monitor their behaviour. Location of the company is irrelevant. A US software company serving Thai customers, a European SaaS provider with Thai users, or a Chinese e-commerce platform serving Thai buyers all fall under the PDPA.

III. Data Controllers vs. Data Processors

Section 6 defines the controller as the person with power to decide on collection, use or disclosure, and the processor as the one acting on the controller's orders. The split decides who owes what: Section 37 places the security and breach-notification duties on the controller, while Section 40 sets out the processor's own duties.

One of the most important distinctions in the PDPA is between a *data controller* and a *data processor*. Understanding this distinction is critical because the obligations differ significantly.

A **data controller**³ is a person or organization that decides *why* personal data is collected and *how* it is used. The controller determines the purposes and means of processing. Typically, this is your company, the business that benefits from the data. Controllers bear the primary compliance burden under the PDPA.



A **data processor**⁴ is a person or organization that processes personal data on behalf of, and on the instructions of, a controller. A processor does not decide why or how the data is used; it merely carries out the controller's instructions. Examples include cloud service providers, payment processors, and data analytics vendors.

If your company is a controller, you must obtain a lawful basis for processing (discussed below) and comply with data subject rights requests. If you are a processor, your obligations are primarily contractual, you must ensure that your processing adheres to your contract with the controller and implement appropriate security measures. A processor cannot legally process data for purposes other than those specified by the controller.

In practice, a company may be both a controller and a processor at different times. For example, a human resources consultancy may be a processor when it processes payroll data on behalf of an employer (controller), but a controller when it uses that anonymized data for its own research or business intelligence.

IV. Six Lawful Bases for Processing Personal Data

Section 19 makes consent the starting point: without it a controller may not collect, use or disclose personal data. Section 24 then lists six grounds that displace the need for consent, archiving and research, vital interests, contract, public task, legitimate interests, and legal obligation. Every processing activity needs consent or one of those six.

Before you can collect or use personal data, you must have a *lawful basis* for doing so. Consent is the default rule: under Section 19 the controller may not collect, use or disclose personal data without the data subject's consent. Section 24 then sets out six grounds on which personal data may be collected *without* consent.⁵ A controller must be able to point to consent or to one of those grounds for each processing activity; without either, the processing is unlawful.



Where consent is relied on, it must be requested explicitly, separately from other matters, and in plain language. It should be freely given and not made a condition of a service that does not need the data, and the data subject may withdraw it at any time, as easily as it was given.⁶ The six grounds in Section 24 that apply without consent are:

1. Archives, Research or Statistics, Processing serves the preparation of historical documents or archives in the public interest, or research or statistics, with suitable safeguards as prescribed by the Committee (Section 24(1)).

2. Performance of a Contract, Processing is necessary to perform a contract with the data subject, or to take steps at the subject's request before entering into a contract. For example, an e-commerce platform may process an address and payment details because processing is necessary to fulfil the purchase order.

3. Vital Interests, Processing is necessary to protect the vital interests of the data subject or another person. This is a narrow exception used in life-or-death situations, such as processing medical data to save someone's life in an emergency.

4. Legitimate Interests⁷, Processing is necessary for the legitimate interests of the controller or a third party, provided those interests are not overridden by the rights and freedoms of the data subject. This basis requires a balancing test: you must weigh your business interest against the privacy expectations of the individual.

5. Compliance with Legal Obligations, Processing is required by law. For example, an employer must process employee tax identification numbers because Thai tax law requires tax on wages to be withheld and reported.

6. Public Task, Processing is necessary for the performance of a public task or governmental function. This basis is typically used by government agencies and public bodies, not by private companies.



Each lawful basis has different requirements and implications. Consent is straightforward but can be withdrawn at any time. Legitimate interests is flexible but requires careful documentation and justification. Controllers should map each processing activity to a specific lawful basis and be prepared to explain why that basis applies if challenged by the Personal Data Protection Committee (PDPC), Thailand's data protection authority.

V. Sensitive Personal Data: The Stricter Category

Section 26 prohibits collecting sensitive data without explicit consent and names the categories itself: racial or ethnic origin, political opinions, cult, religious or philosophical belief, sexual behaviour, criminal records, health data, disability, trade union information, genetic and biometric data, plus a catch-all the Committee may extend.

Not all personal data is treated equally under the PDPA. *Sensitive personal data* receives heightened protection. Section 26 both lists the sensitive categories and prohibits their collection without the data subject's *explicit* consent, subject to narrow exceptions.⁸⁹

Section 26 names racial or ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic data and biometric data, and closes with a catch-all for any other data that may affect the data subject in the same manner, as prescribed by the Committee. The list is therefore open, not fixed.

The core rule: collection of sensitive data generally requires explicit consent. Unlike ordinary personal data, which may be collected based on other lawful bases, sensitive data almost always requires the data subject to have actively and explicitly agreed to collection. This consent must be specific to the type of sensitive data and the purpose. It cannot be buried in a terms-of-service checkbox.



The exceptions in Section 26 are limited. They include cases where: (a) the data subject is unable to give consent (e.g., unconscious in a hospital), and processing is vital to the subject's interests; (b) processing is necessary for a public health purpose; (c) processing is necessary to pursue a legal claim; or (d) processing is necessary for purposes of archiving, scientific research, or historical or statistical purposes.

For many foreign businesses, the key takeaway is this: avoid collecting sensitive data unless absolutely necessary. If you must collect it (e.g., health data for an insurance platform, or criminal records for a background-check service), obtain explicit written consent and implement robust security measures.

VI. Eight Rights of Data Subjects

Sections 30 to 36 give the data subject a working set of rights: access and a copy, portability, objection, erasure or anonymisation, restriction of use, and correction. Section 30 paragraph four is the operative deadline, an access request that cannot lawfully be refused must be met without delay and within thirty days of receipt.

The PDPA grants data subjects the eight rights below. Controllers should respond to requests promptly; for access requests, Section 30 paragraph four sets a limit of thirty days from receipt.

- 1. Right of Access (Section 30)¹⁰**, A data subject may request access to any personal data relating to them that the controller holds, and obtain a copy of it, or ask the controller to disclose how it obtained data collected without the data subject's consent.
- 2. Right to Correction and Completion (Sections 35-36)¹¹**, A data subject may request that inaccurate or incomplete data be corrected or completed.
- 3. Right to Deletion/Right to Be Forgotten (Section 33)¹²**, A data subject may request deletion or destruction of their personal data, or anonymization, when the data is no longer necessary for its original purpose or when consent is withdrawn.



4. Right to Data Portability (Section 31)¹³, A data subject may request their personal data in a commonly used, machine-readable format (such as CSV or XML) and request that the controller transmit it to another controller.

5. Right to Object (Section 32)¹⁴, A data subject may object to processing, particularly when the controller relies on legitimate interests or direct marketing.

6. Right to Restriction of Processing (Section 34)¹⁵, A data subject may request that processing be temporarily suspended, for example, while the accuracy of data is being verified or while a dispute is being resolved.

7. Right to Withdraw Consent (Section 19), A data subject may withdraw consent at any time, as easily as it was given, unless withdrawal is restricted by law or by a contract that benefits the data subject. Withdrawal does not affect processing already carried out lawfully on the basis of that consent.

8. Right to Lodge a Complaint (Section 73), A data subject may file a complaint where a controller or processor, or their employees or contractors, breaches the Act or a notification issued under it. Complaints are considered by an expert committee appointed under the Act.

Foreign companies must establish processes to respond to these requests. This means implementing systems to locate and retrieve personal data, procedures to verify the identity of requesters, and timelines to respond. Large-scale operations should designate a Data Protection Officer (DPO) or establish a dedicated team to manage subject access requests and other rights inquiries.

VII. Cross-Border Data Transfers

Section 28 permits a transfer abroad only where the destination has an adequate protection standard measured against rules the Committee prescribes under Section 16(5), or where one of six listed exceptions applies. Section 29 offers the alternative route for transfers inside the same affiliated business under an approved data protection policy.



The PDPA restricts the transfer of personal data outside Thailand's borders. Section 28 provides the framework, and Section 29 governs transfers within the same affiliated business or group of undertakings.¹⁶ Data may be transferred abroad only if:

(a) The destination country has an *adequate level of protection* as determined by the Personal Data Protection Committee, or (b) Appropriate *safeguards* are in place, such as standard contractual clauses or binding corporate rules.

The Act does not itself name any adequate jurisdiction: adequacy is determined against the rules prescribed by the Committee under Section 16(5), and where adequacy is in doubt the question goes to the Committee under Section 28 paragraph two, whose decision may be revisited on new evidence. In practice, a controller transferring data to a country it cannot show to be adequate should rely on one of the six exceptions in Section 28 or, for transfers inside its own group, on a personal data protection policy under Section 29, backed by contractual safeguards that impose PDPA-equivalent obligations on the recipient.

VIII. Thailand's PDPA vs. the EU's GDPR: Key Differences

The PDPA was drafted on the GDPR's template and matches it on extraterritorial reach and on the shape of the lawful bases, but diverges sharply on money. GDPR Article 83 reaches EUR 20 million or 4% of worldwide turnover; the PDPA's ceiling is 5 million baht under Section 84, and only for sensitive-data breaches.

The PDPA was largely modelled on the EU's General Data Protection Regulation (GDPR),¹⁷ which entered force in 2018. Understanding the differences is important for companies subject to both laws.

Territorial Scope: Both laws have extraterritorial reach.¹⁸ Both apply to organizations outside the jurisdiction that offer goods or services or monitor behaviour of residents.

Consent Mechanism: Both require explicit, informed, freely given consent for most processing. Both recognize that consent must be freely given and easily withdrawn.



Lawful Bases: The PDPA's consent rule and the six grounds in Section 24 closely track Article 6 of the GDPR. Both recognize consent, contract, legal obligation, vital interests and public task, and both include a legitimate interests basis that requires balancing. The PDPA also lists archives, research and statistics as a separate ground.

Sensitive Data: The PDPA's sensitive categories under Section 26 largely track the GDPR's special categories. Both impose heightened restrictions.

Data Subject Rights: Both regimes grant rights of access, correction, erasure, portability, objection and restriction, the right to withdraw consent, and the right to lodge a complaint. The GDPR adds a specific right concerning decisions based solely on automated processing (Article 22), which the PDPA does not contain.

Penalties, Major Difference: The GDPR imposes fines of up to EUR 20 million or 4% of total worldwide annual turnover, whichever is higher, for the most serious infringements.¹⁹ The PDPA's administrative fines are tiered and capped at 5 million baht, and that ceiling applies only to sensitive-data breaches under Section 84, roughly EUR 130,000.²⁰ This represents a significant gap in financial deterrence.

The bottom line: if you operate in both jurisdictions, compliance with the GDPR will largely put you in compliance with the PDPA, but not vice versa.

IX. Penalties

Penalties run on three tracks. Administrative fines are tiered at one, three and five million baht under Sections 82, 83 and 84. Section 79 adds imprisonment of up to one year and a fine of up to one million baht where sensitive data is misused for unlawful gain. Civil damages sit on top of both.

Violations of the PDPA carry administrative, criminal, and civil consequences.



Administrative Fines: The ceiling depends on the duty breached: up to 1 million baht under Section 82 (notice, records, DPO and consent-form duties), up to 3 million baht under Section 83 (including the lawful-basis, cross-border and controller-duty provisions), and up to 5 million baht under Section 84 for breaches concerning sensitive data.²⁰ Each violation is a separate offence, so fines can accumulate rapidly.

Criminal Penalties: A controller that uses or discloses sensitive personal data without consent (Section 27) or transfers it abroad in breach of Section 28 in a manner likely to cause damage faces imprisonment of up to six months, a fine of up to 500,000 baht, or both; where this is done to obtain an unlawful benefit for itself or another person, the penalty rises to imprisonment of up to one year, a fine of up to 1 million baht, or both. These offences are compoundable.²¹

Civil Liability: Data subjects may sue controllers or processors for damages, including non-patrimonial (moral) damages. A company that mishandles data may face claims for injury to reputation, emotional distress, or loss of opportunity.

X. Practical Checklist for Foreign Businesses

Compliance is a documentation exercise before it is a technical one. Map the data, record whether consent under Section 19 or a ground under Section 24 supports each activity, publish a Section 23 notice in Thai and English, build a thirty-day process for Section 30 requests, and test every transfer against Section 28.

To comply with the PDPA, foreign businesses should:

1. **Conduct a Data Audit,** Map all personal data your company collects, stores, and processes relating to Thai residents. Identify the lawful basis for each processing activity.
2. **Obtain Lawful Basis Documentation,** Document why each processing activity is necessary and which of the six lawful bases applies. If relying on legitimate interests, conduct and document a balancing test.



3. **Update Privacy Notices**, Publish a transparent privacy policy in Thai and English that explains what data you collect, why, how long you keep it, and the rights of data subjects.
4. **Implement Data Subject Rights Procedures**, Establish a process to respond to access requests, deletion requests, objections, and other rights inquiries within 30 days.
5. **Review Consent Mechanisms**, If you rely on consent, replace pre-ticked boxes with clear, affirmative consent for each purpose. Allow easy withdrawal of consent.
6. **Assess Sensitive Data Handling**, If you collect any category of sensitive data under Section 26, obtain explicit consent and implement heightened security measures.
7. **Review Vendor Contracts**, Ensure your contracts with processors (cloud providers, vendors, payment processors) include PDPA-compliant data protection terms. Your company remains liable if a processor violates the PDPA.
8. **Implement Security Measures**, The PDPA requires "reasonable" measures to protect data against unauthorized access, disclosure, alteration, and destruction. This includes encryption, access controls, employee training, and incident response procedures.
9. **Draft a Breach Notification Plan**, Have a process in place to notify affected parties and regulators if a data breach occurs.
10. **Monitor PDPC Guidance**, The Personal Data Protection Committee issues guidance and enforcement decisions regularly. Stay informed about evolving standards and adjust your practices accordingly.

For many foreign companies, compliance with the PDPA is not as complex as compliance with the GDPR, but the law's extraterritorial reach means it applies to you if you serve Thai customers. Taking these steps now will minimize legal risk and protect your company's reputation.



Footnotes

1. Personal Data Protection Act B.E. 2562 (2019), Royal Gazette Vol. 136, Part 69a, 27 May 2019. The Act came into full effect on 1 June 2022 following a series of postponements prompted by COVID-19 and the need for businesses to prepare. [พ.ร.บ.นี้ผ่านการประกาศมาตั้งแต่ปี 2562 แต่มีการเลื่อนบังคับใช้หลายครั้งจนมีผลจริงในปี 2565]
2. Section 5, paragraph two PDPA, extraterritorial reach: where a data controller or data processor is outside Thailand, the Act applies to the collection, use or disclosure of personal data of data subjects who are in Thailand, where the activities are (1) the offering of goods or services to data subjects in Thailand, irrespective of whether payment is made, or (2) the monitoring of the data subject's behaviour, where the behaviour takes place in Thailand. [ขอบเขตนอกราชอาณาจักร, บริษัทต่างชาติที่ขายสินค้า/บริการให้คนไทย หรือติดตามพฤติกรรมคนไทย ต้องปฏิบัติตาม PDPA เช่นกัน]
3. Section 6 PDPA, "Personal Data Controller": a person or juristic person having the power and duties to make decisions regarding the collection, use, or disclosure of personal data. [ผู้ควบคุมข้อมูล คือคนที่ตัดสินใจว่าจะเก็บ ใช้ หรือเปิดเผยข้อมูลอย่างไร]
4. Section 6 PDPA, "Personal Data Processor": a person or juristic person who operates in relation to the collection, use, or disclosure of personal data pursuant to the orders given by or on behalf of a controller. [ผู้ประมวลผลทำงานตามคำสั่งของผู้ควบคุม เช่น บริษัท cloud storage]
5. Section 24 PDPA, collection without consent is permitted only where: (1) it is for the preparation of historical documents or archives in the public interest, or for research or statistics with suitable safeguards; (2) it is to prevent or suppress a danger to a person's life, body or health; (3) it is necessary for the performance of a contract to which the data subject is a party, or to take steps at the data subject's request before entering a contract; (4) it is necessary for a task carried out in the public interest, or for the exercise of official authority vested in the controller; (5) it is necessary for the legitimate interests of the controller or another person, except where overridden by the data subject's fundamental rights; (6) it is necessary for compliance with a law to which the controller is subject. [ม.24, กฎฐานที่เก็บข้อมูลได้โดยไม่ต้องขอความยินยอม]
6. Section 19 PDPA, consent must be requested explicitly, in writing or by electronic means, separately from other matters, in language that is easily accessible and understandable; the data subject may withdraw consent at any time and withdrawal must be as easy as giving it. [ความยินยอมต้องชัดเจน เจาะจงวัตถุประสงค์]
7. Section 24(5) PDPA, legitimate interests: collection without consent is permitted where necessary for the legitimate interests of the controller or of another person or juristic person, except where such interests are overridden by the fundamental rights of the data subject. [ฐานประโยชน์อันชอบธรรม]
8. Section 26 paragraph one PDPA, sensitive personal data: racial or ethnic origin, political opinions, cult, religious or philosophical beliefs, sexual behaviour, criminal records, health data, disability, trade union information, genetic data, biometric data, or any data which may affect the data subject in the same manner as prescribed by the Committee. Section 23 is a different provision: it is the controller's duty to inform the data subject of the purpose and details of collection. [ม.26, ข้อมูลอ่อนไหว]
9. Section 26 PDPA, collection of sensitive data generally requires explicit consent; limited exceptions include vital interests where the data subject is unable to give consent, public interest in public health, archiving for scientific/historical/statistical purposes, and legal claims. [ข้อมูลอ่อนไหวต้องได้รับความยินยอมโดยชัดแจ้ง]



10. Section 30 PDPA, right of access: the data subject has the right to request access to and obtain a copy of personal data relating to them. [สิทธิขอข้อมูล]
11. Section 35 PDPA, the controller must keep personal data accurate, up to date, complete and not misleading; Section 36 governs what happens where the controller declines to act on the data subject's request to comply with Section 35, requiring the request and the reasons for refusal to be recorded under Section 39. [ม.35-36, สิทธิขอแก้ไขข้อมูลให้ถูกต้อง]
12. Section 33 PDPA, right to erasure (right to be forgotten): the data subject may request deletion or destruction of their personal data, or de-identification, when the data is no longer necessary for its purpose or consent has been withdrawn. [สิทธิขอลบข้อมูล]
13. Section 31 PDPA, right to data portability: the right to receive personal data in a commonly used and machine-readable format and transmit it to another controller. [สิทธิโอนข้อมูล]
14. Section 32 PDPA, right to object: the data subject may object to the collection, use, or disclosure of their personal data at any time. [สิทธิคัดค้าน]
15. Section 34 PDPA, right to restriction of processing. [สิทธิระงับการใช้ข้อมูล]
16. Section 28 PDPA, cross-border transfer: the destination country or international organisation must have an adequate data protection standard and the transfer must follow the rules prescribed by the Committee under Section 16(5), except in six cases (compliance with the law; informed consent to the inadequate standard; performance of a contract with the data subject; a contract made in the data subject's interest; preventing danger to life, body or health where consent cannot be given; substantial public interest). A dispute over adequacy is decided by the Committee under Section 28 paragraph two. Section 29 covers intra-group transfers under an approved personal data protection policy. Section 37, by contrast, sets out the controller's general duties, including security measures. [ม.28-29, การส่งข้อมูลออกนอกประเทศ]
17. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data [2016] OJ L 119/1 (GDPR). [กฎหมายคุ้มครองข้อมูลของสหภาพยุโรป]
18. GDPR Article 3, territorial scope: applies to any organisation worldwide that offers goods/services to EU residents or monitors their behaviour, regardless of where the organisation is established. Compare Section 5, paragraph two PDPA. [GDPR มีขอบเขตนอกอาณาเขตเช่นกัน]
19. GDPR Article 83(4)-(5), administrative fines of up to EUR 20 million or 4% of total worldwide annual turnover, whichever is higher, for the most serious infringements. Compare Sections 82-84 PDPA: administrative fines of up to THB 1, 3 or 5 million depending on the duty breached. [โทษปรับของ GDPR สูงกว่า PDPA ไทย]
20. Sections 82-84 PDPA, administrative fines: up to THB 1 million under Section 82; up to THB 3 million under Section 83 (breach of Sections 21, 22, 24, 25 para 1, 27, 28, 32 para 2 or 37, or consent obtained by deception); up to THB 5 million under Section 84 for breaches relating to sensitive data under Section 26. Each unlawful act is a separate offence. [ม.82-84, โทษปรับทางปกครอง 1/3/5 ล้านบาท]
21. Section 79 PDPA, criminal penalties: a controller that breaches Section 27 paragraph one or two, or fails to comply with Section 28, in relation to sensitive personal data under Section 26, in a manner likely to cause another person damage, loss of reputation, contempt, hatred or humiliation, is liable to imprisonment of up to six months, a fine of



up to THB 500,000, or both (paragraph one); where this is done to obtain an unlawful benefit for oneself or another person, the penalty is imprisonment of up to one year, a fine of up to THB 1 million, or both (paragraph two). The offences are compoundable (paragraph three). [ม.79, โทษอาญาเกี่ยวกับข้อมูลอ่อนไหว]

