Jurisdictional Report
KINGDOM OF THAILAND

Reporter: **David Duncan**
Consultant, Tilleke & Gibbins

A INTRODUCTION

1 Thailand lacks a comprehensive data privacy regime, in the form of what would typically be encountered in major jurisdictions overseas. However, many commentators have erroneously asserted that Thai law contains no provisions of relevance to data privacy. Indeed, the Constitution reflects the concept that people's privacy should be respected and that personal data should not be exploited, and there are general provisions of law that could be used in relation to a wrongful disclosure of one's personal data that causes damage (*ie*, a tort) or in the case such would amount to criminal defamation. Beyond those general provisions, data privacy provisions exist in several other areas of law, such as sector-specific regulations or licence conditions, in provisions setting out protections for certain categories of information, or in requirements specific to certain professions.

2 A Personal Data Protection Bill has been pending in various forms for at least 15 years, which would establish a personal data protection regime that would feature many of the characteristics with which Western data privacy practitioners are accustomed. While many have speculated as to why the Bill has not been enacted, the reality is that there are likely numerous reasons, such as legislative prioritisation, a general lack of concern about personal data protection among the population, and concern about possible disruption to business and investment that may be brought about by a burdensome new regulatory regime. However, as noted elsewhere herein, progress is being made, and the most recent version of the Bill strikes a good balance between legitimate privacy concerns and not being overly burdensome to business.

3 Despite the lack of a conventional data privacy framework at present, cross-border data transfers still occur with regularity. In most

cases, these are simply a function of economics and business, as well as the efficiencies brought about by centralised hosting and cloud services. In practical terms, businesses in Thailand do not face significant difficulties in relation to cross-border data transfers.

B GENERAL LEGAL FRAMEWORK OF INTERNATIONAL DATA TRANSFERS

i *Existing data privacy protections in national legislation*

4 As noted, Thailand lacks a comprehensive data privacy regime, but a Bill to provide for one has been pending for more than 15 years. One of the more recent versions is available on the website of the Council of State, and another even more recent version is available on the Thai government's public consultation website.

5 Were it to be enacted as written in this most recent draft, cross-border data transfers would be addressed in its sections 13(5) and 24, translations of which are as follows:

> **Section 13** The Personal Data Protection Commission has the power as follows
>
> …
>
> (5) to announce and impose criteria to protect the delivery of personal information sent or transferred abroad
>
> …
>
> **Section 24** In the case the person who controls the personal information sends or transfers personal information abroad, such person is required to comply with the criteria on personal information protection as prescribed by the Commission according to Section 13(5), except:
>
> (1) where the law requires;
> (2) where consent is received from the owner of the personal information;
> (3) to comply with a contract between the owner of the personal information and the controller of the personal information;
> (4) to protect the benefit of the owner of the personal information who cannot give consent at that time;
> (5) to transfer to a person who received a standard certificate mark to protect the information in accordance with Section 32 or Section 34; or
> (6) others as imposed in regulations.

6 In February 2018, a period of public consultation in respect of the Bill concluded. Over the past years, it has been under the consideration of the Ministry of Information Communications Technology (now the Ministry of Digital Economy and Society), the Office of the Official Information Commission, the Council of State and the Cabinet. Virtually all of the drafts have contemplated the creation of a new Personal Data Protection Commission, but there have been differences in the entity that would function as Thailand's personal data protection authority, whether building the Office of Official Information Commission into a full-fledged data protection regulator, assigning such authority to the forthcoming Office of National Cybersecurity Committee or the Electronic Transactions Development Agency, or building an entirely new agency for that purpose. The most recent draft contemplates that the Office of the Personal Data Protection Commission would be a newly established agency (see below).

7 Meanwhile, in the general case, data privacy is addressed in several general provisions of statute. The Constitution (2017) also addresses personal data protection in its section 32, a translation of which is as follows:

> **Section 32** A person shall enjoy the rights of privacy, dignity, reputation and family.
>
> An act violating or affecting the right of a person under paragraph one, or an exploitation of personal information in any manner whatsoever shall not be permitted, except by virtue of a provision of law enacted only to the extent of necessity of public interest.

8 Moreover, provisions of the Civil and Commercial Code address liability in respect of wrongful acts pertaining to personal data. The following are translations of relevant provisions:

> **Section 420** A person who, wilfully or negligently, unlawfully injures the life, body, health, liberty, property or any right of another person, is said to commit a wrongful act and is bound to make compensation therefore.
>
> **Section 423** A person who, contrary to the truth, asserts or circulates as a fact that which is injurious to the reputation or the credit of another or his earnings or prosperity in any other manner, shall compensate the other for any damage arising therefrom, even if he does not know of its untruth, provided he ought to know it.

A person who makes a communication the untruth of which is unknown to him, does not thereby render himself liable to make compensation, if he or the receiver of the communication has a rightful interest in it.

9 A wrongful disclosure of personal information could also amount to defamation, under the Penal Code:

Section 326 Whoever imputes anything to another person before a third person in a manner likely to impair the reputation of such other person or to expose such other person to hatred or contempt is said to commit defamation, and shall be punished with imprisonment not exceeding one year or fine not exceeding THB 20,000, or both.

Section 327 Whoever imputes anything to a deceased before a third person, and such imputation is likely to impair the reputation of the father, mother, spouse, or child of the deceased or to expose such person to hatred or contempt, is said to commit defamation, and shall be liable to the same punishment as provided in Section 326.

Section 328 If the offence of defamation is committed by means of publication of a document, drawing, painting, cinematograph film, picture, or letters made visible by any means, gramophone record, or another recording instrument, recording picture or letters, or by broadcasting or spreading a picture, or by propagation by any other means, the offender shall be punished with imprisonment not exceeding two years and fine not exceeding THB 200,000.

Section 329 Whoever, in good faith, expresses any opinion or statement:

(1) by way of self-justification or defence, or for the protection of a legitimate interest;
(2) in the status of being an official in the exercise of his functions;
(3) by way of fair comment on any person or thing subjected to public criticism; or
(4) by way of fair report of the open proceedings of any Court or meeting, shall not be guilty of defamation.

Section 330 In case of defamation, if the person prosecuted for defamation can prove that the imputation made by him is true, he shall not be punished, but he shall not be allowed to so prove if such imputation concerns personal matters, and such proof will not be of benefit to the public.

…

> **Section 332** In case of defamation in which judgment is given that the accused is guilty, the Court may order:
>
> (1) to seize and destroy the defamatory matter or part thereof;
>
> (2) to publish the whole or part of the judgment in one or more newspapers once or several times at the expense of the accused.
>
> **Section 333** The offences in this Chapter are compoundable offences. If the injured person in the defamation dies before making a complaint, the father, mother, spouse, or child of the deceased may make a complaint, and it shall be deemed that such person is the injured person.

10 Similar provisions exist in the Computer Crimes Act BE 2550 (as amended). These translate as follows:

> **Section 16** Any person who brings into a computer system accessible by the public computer data which appears to be a photograph of another person, where such photograph has been created, edited, supplemented, or modified by an electronic means or any other means, in a manner likely to cause that other person to be defamed, insulted, hated, or embarrassed, shall be liable to imprisonment for a term not exceeding three years and to a fine not exceeding THB 200,000.
>
> If the act under paragraph one is committed against a photograph of the deceased and such act is likely to cause the deceased's parent, spouse, or child to be defamed, insulted, hated, or embarrassed, the perpetrator shall be liable to the same penalty as that provided in paragraph one.
>
> If the act under paragraph one or paragraph two subsists in the bringing into a computer system in good faith, which constitutes a fair comment on any person or matter which is ordinarily made by a member of the public, the perpetrator shall not be guilty.
>
> The offences under paragraph one and paragraph two are compoundable offences.
>
> If the injured person for the offence under paragraph one or paragraph two dies before making a complaint, the parent, spouse, or child of the injured person shall be entitled to make a complaint and shall be deemed to be the injured person.

11 Certainly, these provisions are not specific to data transfers. Indeed, they apply far more broadly. Nevertheless, they can be applied in relation to data transfers that are wrongful or that constitute criminal offences.

12 Going beyond the general case, data privacy provisions exist in several other areas of law, such as sector-specific regulations or license conditions, in provisions setting out protections for certain categories of information, or in requirements specific to certain professions, for example:

(a) Chapter 4 ("Protection for Information Subject") of the Credit Information Business Act BE 2545 (as amended) (as relevant to credit bureaus);

(b) Regulations applicable to telecommunications licensees under the Telecommunications Business Act BE 2544 (as amended), section 50 of which provides that the National Broadcasting and Telecommunications Commission is to *establish measures for user protection concerning personal data, right to privacy and freedom to communicate by means of telecommunications*;

(c) provisions of the National Health Act BE 2550 (as amended) (as relevant to personal health information);

(d) provisions of the Financial Institutions Business Act BE 2551 (as amended) (as relevant to banks, credit fonciers, and finance companies);

(e) conditions of licences issued under the Securities and Exchange Act BE 2535 (as amended) (as relevant to securities companies); and

(f) conditions of notifications made and licences and registrations issued under the Royal Decree on Control and Supervision of Electronic Payment Service Business BE 2551, section 16(1) of which empowers the Electronic Transactions Commission to prescribe rules, procedures and conditions on custody and disclosure of the personal information of the service users (as relevant to electronic payment licensees), being replaced by the Payment Systems Act BE 2560.

13 Given the various other data protection obligations that are already in effect in many important sectors of the economy, the Personal Data Protection Bill contains provisions to address how the Bill (once enacted) would function in co-ordination with pre-existing laws and regulations.

ii *International commitments*

14 Thailand is party to a host of treaties and international agreements. Among these, Thailand has ratified the International Covenant on Civil and Political Rights, but it has not signed either of the two Optional Protocols. Thailand is also involved in a number of free trade agreements ("FTAs"), both bilateral and multilateral, and some of these contain very general provisions on personal data protection. The following is an example from the Thai-Chile FTA:

> **Article 11.7: Electronic Commerce**
>
> 1. Recognizing the global nature of electronic commerce, the Parties shall endeavour to:
>
> …
>
> (j) take appropriate measures and take into account international standards on personal data protection:
>
> (i) notwithstanding the differences in existing systems for personal data protection in the territories of the Parties, each Party shall take such measures as it considers appropriate and necessary to protect the personal data of users of electronic commerce; and
>
> (ii) in the development of data protection standards, each Party shall, to the extent possible, take into account international standards and the criteria of relevant international organizations …

15 However, treaties and international agreements are not self-executing under Thai law. Rather, implementing legislation is required.

16 Thailand is a member of the Asia-Pacific Economic Cooperation ("APEC"), but Thailand does not participate in the APEC Cross-border Privacy Enforcement Arrangement, nor has Thailand joined the APEC Cross-Border Privacy Rules system.

17 Thailand is a member of the Association of Southeast Asian Nations ("ASEAN") Economic Community. The ASEAN Framework on Personal Data Protection is among the reasons that Thailand has been pursuing the Personal Data Protection Bill, though the Bill predates the Framework by several years.

18 Thailand is not an observer on the Consultative Committee of the Council of Europe Convention 108, and it has not been recognised by the European Union as offering an adequate level of protection on application of Article 25(6) of Directive 95/46/EC. While the European General Data Protection Regulation ("GDPR") does not have the force or effect of law in Thailand, there are a number of European companies with operations in Thailand, which makes the GDPR relevant in Thailand, in some situations.

iii *Role of privacy enforcement authority*

19 At this stage, Thailand lacks a comprehensive privacy enforcement authority ("PEA"). Whilst some sector-specific authorities, such as the Bank of Thailand, the Securities and Exchange Commission, and the National Broadcasting and Telecommunications Commission, have regulatory purview including personal data protection matters within their respective economic sectors, personal data protection is not their primary focus. However, the version of the Personal Data Protection Bill which underwent consultation earlier this year would, if enacted, provide for the creation of a Personal Data Protection Commission, an Office of the Personal Data Protection Commission, and a Committee of the Office of the Personal Data Protection Commission. Collectively, they would have a wide array of powers. Among these, the Commission would have the authority to impose conditions for the protection of personal data sent or transferred overseas (section 13(5)) and to settle relevant breaches (section 75). Regarding international co-operation, the Office of the Personal Data Protection Commission would, among its powers, have the authority to enter into agreements and cooperate with other organisations, in Thailand and abroad, as relate to the exercise of its powers and duties (section 36(9) of the Bill).

C DEFAULT POSITION, SCOPE AND TERRITORIAL EFFECT

20 In the general case, the law neither authorises nor prohibits international data transfers. Hence, the default position is that it is advisable to obtain consent from each data subject. However, where special provisions of law are applicable, such as in the case of credit information or personal health information, or where one is a

telecommunications licensee, it would be required to obtain consent prior to transfer, except where law or regulations specify an exception. As for the Personal Data Protection Bill, the version which underwent consultation earlier this year would require personal data controllers to act in conformity with conditions imposed by the Commission under section 13(5), except where an exemption would be applicable (see above).

21 In the general case, the law does not use the terms "controllers", "processors" or "intermediaries", as relevant to personal data. This is because, generally, the applicable provisions of law are not specific to personal data issues. For the same reason, there are no exclusions for data in transit, nor are there any exclusions for anonymised, pseudonymised or encrypted data. In contrast, the Personal Data Protection Bill would clearly define "personal data controller" and "personal data processor", with corresponding implications in terms of regulatory obligations.

22 In general, the question of whether Thai law or foreign law is applicable in particular circumstances is addressed in the Act on Conflict of Laws BE 2481 and the Criminal Code. As relevant to wrongful acts, the Act on Conflict of Laws provides (as translated):

> **Section 15** An obligation arising out of a wrongful act is governed by the law of the place where the facts constituting such wrongful act have taken place.
>
> The foregoing provision does not apply to facts which, having taken place in a foreign country, are not wrongful according to Siamese law.
>
> In no case can the injured party claim compensation or remedies other than those allowed by Siamese law.

23 As relevant to criminal defamation, the Criminal Code provides:

> **Section 5** Whenever any offence is even partially committed within the Kingdom, or the consequence of the commission of which, as intended by the offender, occurs within the Kingdom, or by the nature of the commission of which, the consequence resulting therefrom should occur within the Kingdom, or it could be foreseen that the consequence would occur within the Kingdom, it shall be deemed that such offence is committed within the Kingdom.
>
> In case of preparation or attempt to commit any act provided by the law to be an offence, even though it is done outside the Kingdom, if the

> consequence of the doing of such act, when carried through to the stage of accomplishment of the offence, will occur within the Kingdom, it shall be deemed that the preparation or attempt to commit such offence is done within the Kingdom.
>
> **Section 6** Whenever any offence is committed within the Kingdom, or is deemed by this Code as being committed within the Kingdom, even though the act of a co-principal, a supporter or an instigator in the offence is done outside the Kingdom, it shall be deemed that the principal, supporter, or instigator has committed the offence within the Kingdom.

24 This would apply also in considering criminal offences specified under other Acts, except where those other Acts provide otherwise.

25 Hence, there are many scenarios in which Thai law could apply to data transfers. In theory, it would even be possible that a person abroad whose data were imported into Thailand could avail himself or herself of provisions of Thai law.

D DATA LOCALISATION

26 In the general case, data localisation is not required in Thailand.

27 However, some sector-specific provisions effectively require the storage of some data in covered businesses in Thailand. Examples include licence conditions applicable to electronic payment licensees and regulations applicable to credit bureaus.

E DATA TRANSFER MECHANISMS

28 Given the lack of a comprehensive data privacy regime in Thailand, the data transfer mechanism most frequently used is obtaining consent from each data subject. In the general case, there is no provision for adequacy findings, white lists, binding corporate rules, certifications, trustmarks, privacy seals, codes of conduct or ISO certification, as relevant to data privacy. The most recent draft of the Personal Data Protection Bill contemplates that it would also be permissible for a personal data controller to transfer personal data to recipients that (a) were certified by the Office of the Personal Data Protection Commission as meeting applicable data protection standards (to be

promulgated in regulations); or (b) have received a certification mark from a foreign agency or international organisation that the Personal Data Protection Commission has determined provides for protection equivalent to the requirements under the Thai Personal Data Protection Act. It also leaves open the possibility that additional transfer mechanisms could be permitted by promulgation of ministerial regulations to that effect.

29 As a general matter, it would be helpful for the law to expressly specify situations in which consent of the data subject would not be required, so as to relieve the burden of capturing consent. The Bill does that, to some extent. However, as a practical matter, there is little demand at present for such alternative mechanisms because (a) capturing consent is not too terribly burdensome; and (b) personal data protection is not an area of major interest among the populace.

30 In the general case, a Thai data exporter is not expressly required to have in place legally enforceable obligations regarding the protection of personal data when transferring data overseas. Nevertheless, it remains possible that a Thai data exporter could be liable in respect of a breach by a data importer outside Thailand. For that reason, a Thai data exporter would have natural motivation to protect itself contractually. Standard contractual clauses for data protection matters have not been produced by any government authorities. We have seen some attempts among clients to impose European standard contractual clauses, but such are generally excessive, relative to the current Thai data protection position. Such clauses generally would impose additional obligations and additional liability on a Thai data exporter, relative to what is applicable to the Thai data exporter by virtue of statute.

31 Where sector specific data protection requirements are applicable, some of these specify permissible reasons for transfer of personal data. Examples include those in regulations issued under the Telecommunications Business Act and in provisions of the Credit Information Business Act. However, no such exceptions exist in the general case.