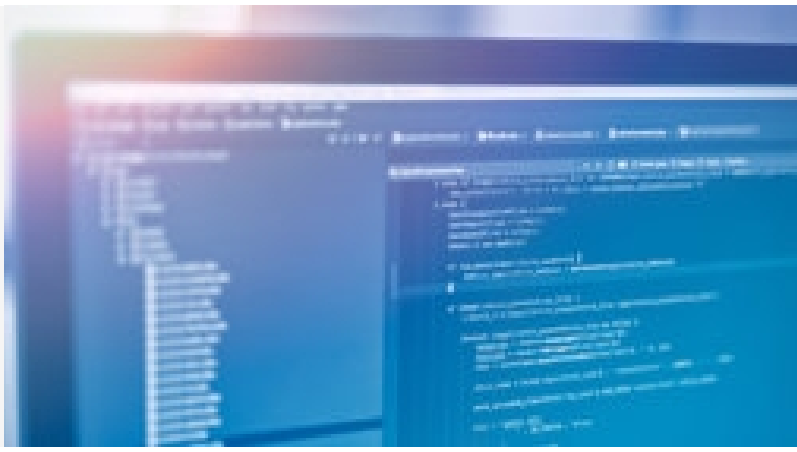
GDPR AND PDPB: WHAT DO YOU NEED TO KNOW ABOUT DATA PRIVACY AND PROTECTION?

10 JULY 2018 • ARTICLE



DATA PRIVACY AND PROTECTION UNDER THAI LAW

Thailand does not have a single law governing data privacy and data protection. We consider below the current draft bill intended to address this. Protection of the right to privacy is contained in the Thai Constitution and s. 420 of the Civil and Commercial Code ("CCC"), which protects individuals from wrongful acts by a person who wilfully, negligently or unlawfully injures the life, body, health, liberty, property or any right of another person. In this context, the disclosure or transfer of data is considered a wrongful act if it causes harm to the data owner.

The Computer Crimes Act (2007) and its 2017 amendments ("CCA") focus primarily on computer and cybercrimes. The CCA prohibits the sending of emails without the ability to opt out and sending emails where the true origin or source of the email is false or not disclosed. The former is comparable with the requirements of General Data Protection Regulation ("GDPR") to obtain the consent of the data owner before processing their data.

A Personal Data Protection Bill ("PDPB") is currently being considered by the Council of State after receiving Cabinet approval in May 2018. The current version contains the following key provisions:

- Data are divided into general personal data, which could directly or indirectly identify an individual, and sensitive personal data, including race, religious beliefs, sexual preferences, medical and criminal records, ethnicity and political views;
- Data controllers are restricted from gathering, using, disclosing or transferring any personal data without the consent of the data owner;
- Data controllers are required to ensure that proper security measures are arranged to protect personal data against any loss, and that the data used or disclosed (when permissible) is correct, complete and current;
- If there is a breach, the data controller must notify the victim immediately and also notify the personal data protection committee in the event of a breach affecting an as yet undefined number of people; and
- Data controllers must obtain consent in writing or by electronic means from the data owner before processing the personal data except as follows:

- Where the data are for research or statistical purposes, provided this is in the public interest and the personal data are anonymised;
- Where the data are for a legitimate purpose for the data controller or a third party; and
- Where the data are to be used in the exercise of official duties or powers or the use of the data is in the public

Breaches of the PDPB will result in a maximum fine of THB500,000 and/or imprisonment not exceeding six months for data controllers and/or a maximum fine of THB1m and/or imprisonment not exceeding two years for data controllers if the offence is committed in order to unlawfully benefit the data controller or another person, or to cause damage to another person. The data controller might also be obliged to reimburse the data owner for any damage caused regardless of intention or negligence.

GDPR

GDPR came into force on 25 May 2018. It applies to personal data, which is information that relates to an identified individual or an individual who can be identified from the information, regardless of whether it is true or accurate. Only completely anonymous data are excluded from the scope of the GDPR. Data which allows for an individual to be indirectly identified would still be subject to the GDPR provided it relates to that individual. To assess whether data relates to an individual, the contents and nature of the data, the purpose of processing the data and the effect on the individual of processing must be considered. As a result, whether data is personal data is an issue for each data controller.

The key requirements are that data must be:

- Processed lawfully, fairly and transparently, on the basis of the legal grounds set out in the GDPR;
- Collected for limited purposes and not further processed beyond those purposes;
- Limited to what is necessary for the processing purposes;
- Accurate and kept up-to-date;
- Kept in a form that permits identification of data subjects for no longer than necessary; and
- Processed in a manner that ensures appropriate security of the personal

Data can only be processed on the following grounds:

- **Consent**: clear consent by the individual to process personal data for a defined purpose;
- **Contract**: processing is necessary to give effect to a contract with an individual;
- **Legal obligation**: processing is required to comply with the law;
- **Vital interests**: processing is required to save the life of an individual;
- **Public task**: processing is required to carry out a public or official duty and this is clearly set out in law; and
- **Legitimate interests**: processing is required for the legitimate interests of the data controller or third

To date, compliance appears to have focussed primarily on ensuring that consent is obtained and individuals are given a clear right to opt out of communication. It is equally important to consider other grounds for data processing, including contractual grounds and legitimate interests. In relation to the latter, this can include commercial interests of the data processor or a third party. It is a crucial that the processing of the data is reasonably expected by the individual and necessary to give effect to the interests. This would appear to include processing the personal data contained on a business card of an individual met at a conference or function, where the legitimate interest of the individual and data processor is to network and use the data to expand their business relationship.

Individuals have the following rights:

- To be informed about the collection and processing of personal data;
- To access within one month of a request for access to the personal data;
- To rectification of incorrect data and completion of incomplete data;
- To erasure of personal data within one month of a request;
- To restrict processing within one month of a request, although this is a limited right;
- To data portability of data provided by an individual to the data controller;
- To object to the use of data for direct marketing and a more limited right in relation to other uses of personal data; and
- In relation to automated decision making and profiling.

To comply with the accountability requirements of the GDPR, companies must have or implement appropriate technical and operational processes and procedures. This can include a data protection policy and code of conduct, having a data protection officer and procedures to deal with breaches of the GDPR and requests from individuals, appropriate data security procedures and protocols and procedures to report breaches of the GDPR.

In the absence of clear consent by an individual, the GDPR also restricts the transfer of personal data out of the EU.

GDPR AND THAILAND

Although GDPR is a regulation of the European Union (“EU”), it has extraterritorial application.

The GDPR will apply to Thai companies with operations in the EU, where personal data is processed in relation to the company’s operations. Thai companies without an EU establishment will also be subject to the GDPR if they process the personal data of EU nationals.

Although the PDPB, if enacted in its current form, would represent a significant improvement in Thai data privacy and protection, it is unlikely to achieve the same levels of protection and privacy as the GDPR. However, if it were to achieve the same or comparable levels of protection, the GDPR does allow the EU to recognise the PDPB as equivalent to the GDPR and, as a result, compliance with the PDPB would be deemed compliant with the GDPR. At this stage, there does not appear to be any consideration of revising the PDPB to achieve comparable levels of protection and privacy as the GDPR.

In the event of a breach of GDPR, EU authorities can impose fines, of up to 4% of annual worldwide turnover or €20m whichever is the greater. It remains to be seen how the EU would enforce payment of these fines against a Thai company without a presence in the EU. This is particularly given the absence of any agreement on the mutual enforcement and recognition of foreign judgments between Thailand and the EU. If the EU sought to enforce a fine against a Thai company, without an EU presence, in the Thai courts, a Thai court is likely to consider whether recognition and enforcement of the fine would be contrary to the public morals and good order of Thailand. The divergence between Thai law, including the PDPB, and the GDPR may provide Thai companies with a persuasive defence to such enforcement and prove a significant hurdle to enforcement.

Thai companies with a presence or operations in jurisdictions with agreements with the EU on the mutual recognition and enforcement of judgments may need to assess the extent to which a fine against the Thai parent or related company could be enforced against a subsidiary or related company in that jurisdiction.

While this may provide some comfort to Thai companies without an EU presence, if the PDPB becomes law, Thai companies will nevertheless be required to ensure that their data processing, storage, use and protection systems and procedures comply with the PDPB. Thai companies may nevertheless be required to comply with GDPR as a precondition to further business dealings with EU customers, suppliers and partners. This is likely to be a condition of tenders, contracts and other agreements. In addition, non-EU customers, suppliers and partners may also require compliance with GDPR to ensure that they comply with the requirements of their EU customers, suppliers and partners.

WHAT DOES THIS MEAN FOR DIRECTORS AND MANAGEMENT OF THAI COMPANIES?

Directors are required to act in the best interests of the company and not to cause the company to suffer harm.

The CCC holds directors of Thai companies personally liable for damages if their acts are not within the scope of their authority and the company's objectives and companies can pursue claims against directors for compensation for harm caused to the company.

In relation to the PDPB, directors and management are responsible for ensuring compliance, including the appointment of an appropriate data controller and ensuring that the data processing, storage, use and protection systems and procedures of the company meet its requirements. Where Thai companies are subject to the GDPR, a similar position will apply, albeit with more stringent requirements than the PDPB.

If the PDPB is implemented as currently drafted, a key issue will be the extent to which breaches are prosecuted and the penalties imposed for breaches. Although the fines in the PDPB appear relatively low by comparison with the penalties in the GDPR, the financial consequences cannot be limited solely to the fines under the PDPB. Companies which are perceived to be weak at enforcing data privacy and protection may suffer a loss of customers and business as a result of a breach, particularly given the increasing volume and nature of data received, processed and stored by Thai companies in the course of their business. Breaches of the PDPB may result in claims against directors and management for failing to ensure that the company had compliant systems, procedures and policies, where this failure is the cause of the harm suffered by the company.

If a company is fined under the GDPR, this creates a more significant financial burden. This in turn will result in greater pressure on the company's directors and management to explain the breaches and address the financial consequences of the fines with their shareholders. Directors and management would then be at greater risk of claims by the company and shareholders arising out of harm suffered by the company as a result of such breaches.

Directors and management may also risk such claims where business is lost as a result of a failure to comply with GDPR, even where there is no legal obligation to do so.

The impact of the PDPB and GDPR is to require boards, directors and management to ensure that they understand their data processing, storage, use and protection systems and procedures and that these comply with these laws and regulations.

Although companies can hire IT and security professionals and delegate implementation and compliance to such employees, this does not reduce or exclude their responsibility to their shareholders for breaches.

Many companies may seek to rely on directors' and officers' insurance policies ("D&O Cover") to protect their directors and management from such claims and to fund the defence of claims and prosecutions. It is important to ensure that companies, directors and management carefully review their D&O Cover to ensure that they understand the extent of cover and the nature and types of exclusions. This is particularly in relation to the costs of defending criminal prosecutions, regulatory investigation and criminal sanctions.

Companies should also ensure that their D&O Cover will address breaches of the PDPB, when enacted, and the GDPR. If the PDPB is enacted as currently drafted, companies and their directors and management should anticipate a higher level of investigation of data protection. The significant changes resulting from the new regime could result in greater awareness of personal data privacy and the consequences of a breach of the PDPB. As a result, companies may then be required to demonstrate that they have appropriate procedures in place to ensure compliance with the PDPB and to deal effectively, promptly and appropriately with any breaches. This will increase the pressure on directors and management to ensure that they have implemented such policies and procedures. Prudent companies, directors and management should also ensure that they have insurance to respond to complaints and claims arising from breaches of the PDPB, including investigation and defence costs.

Companies should also assess the extent to which they have, or can obtain, insurance to cover notification and reporting costs, respond to claims for compensation, the less direct consequences of a breach or a failure to implement compliant procedures and policies, such as loss of reputation. Directors and management should also consider the extent to which they can be held accountable for losses and harm suffered by the company for such indirect consequences and the extent to which D&O Cover will respond on their behalf.

It may also be necessary to have cyber risk insurance or to ensure that an existing cyber risk policy is updated and provides cover commensurate with the increased compliance requirements and consequences of a breach. It may also be necessary to consider the extent to which D&O and cyber risk policies interact and where neither policy may provide insurance cover for certain types of claims.

KEY CONTACT

ALAN POLIVNICK
PARTNER • SYDNEY

T: +61 2 9276 7607

apolivnick@wfw.com