

# Thailand's Personal Data Protection Act – hazards and perils for data holders!

by

*Stephen Frost, Price Sanond*

*Introduction:* Prior to 2019, there was no specific law in Thailand to protect personal data. A person who sought to protect the acquisition, storage or distribution of his/her data had to base an action in contract, or under the doctrine of wrongful act (tort), use certain sections of the Criminal Code, or rely on privacy rights under the constitution. All this has changed with the passing of the Personal Data Protection Act in 2019. The Act is based very much on the European General Data Protection law. Perhaps for this reason, it is unusually long and detailed when compared with other Thai statutes

*Scope of the PDPA:* The PDPA will apply to all persons that receive, store or disclose “data” as defined. Particular measures for compliance will need to be put in place by organisations that receive store or disclose large quantities of data, as part of their normal business activities. The regulatory committee under the PDPA has been appointed but there are a large number of passages in the PDPA where supporting regulations will need to be drafted to clarify duties imposed.

*Exclusions from the Act:* The Act does not apply to collection, use, or disclosure of data for state security, by the mass media, in proceedings in Parliament or the courts or by credit bureaux.

*Territorial scope:* The Act has complex rules where data is collected, stored or used by a Data Controller or Data Processor located outside Thailand.

***Key definitions:*** In the Act,

“*Data*” means any information relating to a person, that enables the person to be identified, directly or indirectly, but excluding information relating to a deceased person.

“*Data Controller*” means a person with power to make decisions regarding the collection, use, or disclosure of data.

“*Data Processor*” means a person who collects, uses, or discloses Data on the orders of a Data Controller, but is not a Data Controller.

In the article below “*dealing in data*” means collecting, using or disclosing it.

***Duties of Data Controllers:*** Except in specified cases, a Data Controller may not deal in data, unless the data subject has consented to this. A request for consent must be in writing or made by electronic means. When making such a request, the Data Controller disclose the purpose of the collection, use or disclosure. A Data Controller may only collect, use or disclose data only for lawful purposes notified to the data subject, prior to or at the time of collection. Subject to certain exceptions, a Data Controller may collect data only from the data subject directly. In certain circumstances, a data subject may request the Data Controller to restrict the use of the data.

**Where the Data Controller need not obtain consent:** The Data Controller need not obtain consent, where:

- (1) it relates to preparation of historical documents or public archives, or for research or statistics, provided measures to safeguard the data subject's rights are put in place
- (2) it is for preventing or suppressing danger to a person's life, body or health
- (3) it is necessary for performance of a contract to which the data subject is a party, or to take steps at the request of the data subject, prior to entering into a contract
- (4) it is necessary for performance of an act carried out in the public interest by the Data Controller, or for the exercising of any authority vested in the Data Controller;
- (5) it is necessary for the legitimate interests of the Data Controller or others, except where such interests are overridden by the rights of the data subject concerning data;
- (6) it is necessary for compliance with a law to which the Data Controller is subject.

**Withdrawal of consent:** Subject to certain conditions, a data subject may withdraw consent to dealing in data at any time. Where such withdrawal affects a data subject, the data controller must notify the data subject of the consequences of withdrawal.

**Minors:** Special rules apply where the data subject is a minor (aged under 20) or is mentally incompetent.

**Data that may not be collected or retained:** Collection of data pertaining to racial, ethnic origin, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health, disabilities, trade union information, genetics, biometrics, or data which may affect the data subject in the same manner, is prohibited without consent from the data subject. Where data collected is no longer required, the Data Controller shall maintain records of the use made of that data.

**Where data controller sends data overseas:** Where the Data Controller sends data outside Thailand, the destination country or international organization that receives the data must in general have adequate data protection standards. Where the Data Controller or Data Processor in Thailand has a data protection policy regarding the transfer of data to a Data Controller or Data Processor outside Thailand, and is in an affiliated business, or the same group of undertakings, if such data protection policy has been certified by the regulator, the transfer of data to that overseas Data Controller or Data Processor can be made.

**Data subject may request copies of data:** A data subject is entitled to copies of data related to him, or to request disclosure of data obtained without his consent. Any request by the data subject shall be complied with within 30 days. The copies supplied must be in readable form.

**Data subject may not object to data dealing:** A data subject may not object to dealing in data where:

(1) the data collected did not require consent, the dealing in data can be shown by the Data Controller to have compelling lawful grounds; or where the dealing in data is for the establishment, compliance or exercise of legal claims, or their defence;

(2) the dealing in such data is for direct marketing;

(3) the dealing in the data is for scientific, historical or statistic research, where necessary in the public interest by the Data Controller.

***Right to request destruction or anonymization of data:*** A data subject may request the Data Controller to erase or destroy the data, or anonymize it, where any of the following applies:

(1) the data is no longer necessary for the purposes for which it was dealt in;

(2) the data subject withdraws consent on which the dealing is based, and the Data Controller has no grounds for such dealing

(3) the data subject objects to the dealing, and the Data Controller cannot oppose such rejection;

(4) the data has been unlawfully dealt in.

Where the Data Controller does not take action as requested, the data subject may request an order from the regulator to compel the Data Controller to take such action.

***Data Controller must ensure accuracy of data:*** The Data Controller must ensure the data remains accurate, up-to-date, complete, and is not misleading.

***Data Controller must record reasons for rejection:*** Where the data subject requests the Data Controller to act, if the latter refuses, it must record the request of the data subject with reasons for the rejection.

***Data Controller's maintenance of records:*** A Data Controller must maintain records of the data collected; the purpose for collection; the period during which the data may be retained, and other records.

***Appointment of Data Protection Officers:*** The Data Controller and Data Processor must appoint a data protection officer in certain cases, with duties as specified under the PDPA.

***Data Protection Committee:*** A Data Protection Committee is established as regulator under the Act. It may investigate complaints made to it under the PDPA, and consider the conduct of Data Controllers. A data subject may complain to the regulator where a Data Controller, a Data Processor or others, do not comply with the PDPA.

***Liability for violation:*** The PDPA impose fines and imprisonment for civil, criminal or administrative violations of the PDPA.

*Price Sanond is a general corporate and commercial law firm. For further information email Stephen Frost at: [sfrost@pricesanond.com](mailto:sfrost@pricesanond.com) or telephone (66) 2 679 1844.*