PERSONAL DATA PROTECTION

Protection of personal data is a major concern in several jurisdictions. Our overseas clients often ask us about their obligations with respect to personal data they may have compiled, whether intentionally or inadvertently, from their employees, customers, clients, or service users. Unfortunately, it is a common misconception that Thai law offers no protection of personal data. In fact, many acts protect personal data and prohibit its disclosure in certain circumstances.

As a foundation, the 2007 Constitution provides that a person's family rights, dignity, reputation and right of privacy shall be protected. The assertion or circulation of a statement or picture in any manner to the public that violates or affects these concepts cannot be made, unless it is beneficial to the public. Personal data shall be protected from those seeking unlawful benefit as provided by law. The coverage of this clause was expanded from the 1997 Constitution.

With respect to personal data maintained by the government, the Official Information Act protects the personal information of Thai people and foreigners resident in Thailand. It defines personal data quite broadly to include information relating to all the particulars of a person, such as education, financial status, health record, criminal record, and employment record that contain the name of a person or a numeric reference, code, or another indication that identifies a person including fingerprints.

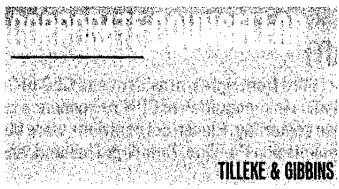
The law specifically includes tapes or discs on which a person's voice is recorded, photographs, and information on those who are deceased. The act sets out requirements for personal data systems operated by the government, establishes restrictions on the disclosure of personal data, and empowers data subjects to request correction of personal data maintained by the government.

The Penal Code also addresses the disclosure of secrets by those who acquire them in the context of their functions as government officials or as practitioners of certain professions, including doctors, pharmacists, midwives, nurses, priests, lawyers, and auditors. Specifically, these individuals are prohibited from disclosing such secrets in a manner likely to cause injury to any person. These obligations also apply to assistants to such professionals, as well as to persons undergoing training for these professions.

There are also a variety of industry-specific regulations. For example, telecommunications licensees are subject to special regulations relating to personal data of their service users, and for procuring the compliance of third parties contracted to process such data. There are also specific requirements that relate to personal data under the Financial Institutions Act, the Credit Information Business Operation Act, and the National Health Security Act.

The Personal Data Protection Bill, which has been under consideration for many years, would provide a comprehensive regulatory structure, applicable to virtually all government and private-sector entities. Based on the latest bill we reviewed, the concept of personal data is essentially the same as that used in the Official Information Act. This bill would establish a Personal Data Protection Board and would set numerous obligations for data controllers. It takes the general approach that a data controller may not collect, use, or disclose any personal data without the consent of the data owner, except as authorised by law. It contains an outright prohibition on collection of data relating to sexual conduct, criminal history, health, national origin, race, political opinion, or religious beliefs, data that are detrimental or impairs one's reputation, or cause any sense of discrimination, or otherwise may be prescribed in ministerial regulations, though it also provides a number of exceptions.

The bill would require that data owners' consent only be sought honestly, and would establish a framework for regulating this. It would also empower data owners to revoke their consent at any time, subject to the requirements of applicable laws and other agreements, though revocation of consent would not be effective with respect to personal data that have been properly made anonymous. Data controllers would also have the obligation to ensure that proper security measures are in place to protect personal data against loss or alteration, and to ensure the data used or disclosed (when permissible) are correct, complete and current. Moreover, if a data controller wishes to use or disclose personal data for a purpose beyond that for which the data owner had given consent, it would usually be necessary to seek further consent. Subject to some exceptions, it would also be necessary to seek consent to transfer personal data overseas, and a process would be established to consider whether the recipient country's personal data protection laws are sufficiently stringent.



Business operators would be subject to additional requirements under the bill. These would include the obligation to set out appropriate policies and to communicate them when seeking consent, to procure the compliance of employees (through terms in employment agreements, as well as through training), to properly identify employees who collect personal data (through name badges), and to file reports with the Personal Data Protection Board. There are also special obligations when winding up a business so that data would still be sufficiently protected or properly disposed. The bill would also establish a certification programme that would allow "good" data controllers to display a certification mark to their customers.

Current laws guard against disclosure of personal data, particularly when such disclosure would be damaging in some way, and higher levels of protection already exist in certain sectors. The Personal Data Protection Bill, when it is enacted, will provide additional protection for consumers, but will also present businesses with greater compliance responsibilities.

This article was prepared by David Duncan, consultant in the Corporate and Commercial Department at Tilleke & Gibbins. Please send comments to Andrew Stoutley at andrew.s@tillekeandgibbins.com