This article was published in the *China Law & Practice (January/February 2014)*.

Decoding the Personal Data Protection Act

Ken-Ying Tseng and Rebecca Hsiao*

Taiwan's Personal Data Protection Act contains several strict provisions relating to written consent requirements that affect foreign companies, even if they are not registered in the jurisdiction

In Taiwan, the collection, processing, and use of personal data by certain regulated entities had, in the past, been subject to the *Computer-processed Personal Data Protection Act* (CPDPA) passed by the legislature and its Enforcement Rules promulgated by the Ministry of Justice (MOJ). On April 27 2010, the legislature passed a bill to amend and rename the CPDPA as the *Personal Data Protection Act* (PDPA). The PDPA and the MOJ's amended Enforcement Rules took effect on October 1 2012 and apply to any person (including any government agency, individual and/or legal entity) that collects, processes or uses personal data in Taiwan. The companies that are subject to the PDPA include those incorporated or registered in Taiwan (including any foreign company which has established a branch office in Taiwan). In addition, any foreign company that collects, processes, or uses an individual's personal data within Taiwan is subject to the PDPA, regardless of whether this foreign company is registered in Taiwan.

Written consent requirements

The PDPA sets out different statutory grounds for legitimate collection, processing and use of personal data. A data subject's written consent is one of the statutory grounds. The written consent requirement can be dispensed with if (i) the collection and processing are specifically permitted by law; (ii) the company and the data subject have entered into or are negotiating a contract; (iii) the data is already in the public domain due to disclosure by the data subject or in a legitimate manner; (vi) the collection and processing are for public interest; or (v) the data has been collected from a source accessible to the company, unless the interest of the data subject takes priority over that of the company.

In addition, a company may use personal data for the specific and lawful purposes for which the personal data has been collected. A company may not use personal data for any other purpose, unless it has obtained the data subject's written consent. The written consent requirement can be dispensed with if (i) such use is specifically permitted by law; (ii) it is to further public interest; (iii) it is to prevent any injury or damage to human life, body, freedom or property; or (iv) it is to prevent any third person's material right or interest from being prejudiced.

Formalities

The CPDPA does not prescribe formalities for the granting of written consent. In the past, a company may even rely on a data subject's deemed consent if it notifies the data subject in writing that it will collect, process or use their personal data for any specific purpose, and the data subject does not object to such collection, processing or use within a reasonable period of time specified in the notification.

Unlike the requirements under the CPDPA, the written consent required under the PDPA is an express and informed consent. In addition, the written consent to the use of personal data for a new purpose should be given separately. A contractual clause in a contract does not constitute the written consent required even if the contract is signed by the data subject. Only a written consent given by a data subject under the following circumstances will be considered a valid consent.

Direct collection

If a company collects personal data directly from a data subject based on their written consent, the company must first notify the data subject of the following information: (i) the company's identity; (ii) the purpose(s) for which the data subject's personal data is collected; (iii) the type of personal data to be collected; (iv) the term, place, and method of use and the people who may use the personal data; (v) the data subject's rights to (a) access his/her personal data to check and review it, (b) have a copy of the personal data, (c) supplement or revise the personal data, (d) demand the company to cease its collection, processing or use of the personal data, and (e) demand the company to delete the personal data; and (vi) consequences of the data subject's failure to provide the required personal data. If a company does not fulfil the aforementioned notification requirement before it obtains a data subject's written consent, this written consent will not be considered valid.

A company is exempt from the above-mentioned notification requirement if (i) it is specifically permitted by law; (ii) the collection is necessary for the performance of job duties provided by law or fulfilment of legal obligations; (iii) notification will prejudice a third party's material interest; or (iv) the data subject already has this information.

Indirect collection

In principle, if a company collects personal data of a data subject indirectly from a third party or other sources based on any of the grounds other than the data subject's written consent, it may inform the data subject of the source of the data and the information stated above in (i) to (v) when it uses such personal data to contact the data subject for the first time. However, if a company collects personal data of a data subject indirectly from a third party based on the data subject's written consent, the company would need to explore a method to fulfil the above notification requirements at the time when the data subject grants the written consent. The local practice is still evolving in this regard. If a company does not fulfil the notification requirement before it obtains a data subject's written consent, it is possible that such written consent will not be considered valid later on.

A company is exempt from the above-mentioned notification requirement if (i) any of the above exemption situations stated in 2.1. exists, (ii) the data subject has disclosed such information by himself/herself or when the information has been publicised legally; or (iii) the notification may not be provided to the data subject or his legal representative.

Use for other purposes

If a company uses the personal data for any other purpose, it must first obtain the data subject's separate written consent. The company must first notify the data subject of the following information: (i) the other purpose(s), (ii) the scope of the use for the other purpose(s), and (iii) how the data subject's rights and/or interests will be affected if he/she chooses not to give his/her consent. If a company prepares a written consent for a data subject to sign in a document that contains other contents, the above-mentioned notification information must be stated in an appropriate place in the document so that the data subject may easily become aware of such information before he/she confirms and consents to the same in writing.

Written consent for marketing

If a company and a data subject (e.g., its client) entered into or are negotiating a contract, the company would anticipate that it may use the data subject's personal data for future marketing purposes. However, the scope of such marketing is unclear. The MOJ (the authorities in charge of establishing the

Enforcement Rules to the PDPA, which define and clarify, among others, terms under the PDPA) has taken a very narrow view on the scope of such marketing, ruling that the products and services that a company promotes for its client should be reasonably related to the contract.

For example, a hotel may collect and process its clients' personal data, when they check in or make online booking registrations, for the purposes of providing room services and fulfilling the hotel's other contractual obligations. The hotel may use the clients' personal data for such purposes, for example, to provide room services. However, according to the MOJ, if the hotel then uses such personal data for analytical or marketing purposes, it will be deemed to be using the personal data for other purposes, and thus must first obtain the clients' written consent. The MOJ emphasised that such a written consent must be an informed written consent. In other words, the hotel must notify its customers of the additional marketing purposes, as well as the other notification items as stated above. Also, based on the PDPA and its Enforcement Rules, such a written consent must be a separate written consent. Given the MOJ ruling, any business in a similar situation has to abide by the additional written consent requirement before it uses its customers' data for promotional campaigns or marketing purposes.

A power supply company in Taiwan sent advertisements of third parties' products and/or services to its clients when issuing electricity bills to them. The power supply company believed that its inclusion of the advertisements in its electricity bills complies with the requirements under the PDPA because it had notified the clients that the conducting of registered businesses (including general advertising services) is one of the purposes for which it collects and processes the clients' personal data. However, according to the MOJ, the power supply company's inclusion of the advertisements of third parties' products and/or services in its electricity bills to its clients based on their power supply contracts does not meet a reasonable expectation of privacy and should not be permitted. The power supply company's inclusion of such third parties' advertisements in its electricity bills to its clients constitutes the use of the clients' personal data for a new purpose other than those for which the clients' personal data had been collected. Hence, the power supply company should have obtained the clients' written consent.

Even if a company has obtained a data subject's written consent for marketing purposes, the data subject still has the right to object to the company's use of their personal data for marketing purpose at any time. Furthermore, when a company contacts a data subject for marketing purposes for the first time, the company must provide the means for the data subject to express their objection and the company must bear any costs or expenses incurred. Once a data subject expresses their objection to the marketing, the company must immediately cease to use their personal data for marketing purposes.

Sharing of personal data

In principle, a company may not share personal data with any third parties for the third parties' marketing purposes or their own benefit, unless the data subject concerned has given written consent. Likewise, a company may not share personal data with its affiliates for the affiliates' marketing purposes or their own benefit, unless the data subject concerned has given written consent.

In a merger, demerger, or assets acquisition transaction conducted in accordance with the *Mergers and Acquisitions Act*, a company may disclose to and provide the acquirer or buyer with the personal data of the data subjects with whom the company has entered into contracts, if the contacts are included in the assets to be transferred by the company to the acquirer or buyer. According to the MOJ, while a company (the seller) may collect, process, and use the personal data based on its contractual relationship with the data subjects, the acquirer or buyer may continue to do the same after the contracts are assigned to it. In these circumstances, the data subjects' written consent is not required.

If a company has legal grounds to collect, process, and use personal data, it may do so by itself or engage a third-party service provider to do the same on its behalf. From the perspective of the PDPA,

the service provider will be deemed an agent commissioned by the company and thus its collection, processing, and use of the personal data will be deemed as that of the company. According to the MOJ, a company does not have to obtain a data subject's written consent in order for the company to legitimately outsource the processing and use of the data subject's personal data to a service provider. However, the company must supervise the service provider to ensure that the latter has appropriate security measures in place and acts in full compliance with the legal requirements as if the company is processing and using the personal data by itself.

*__Ken-Ying Tseng__

Partner

Lee and Li

Ken-Ying Tseng formed and leads the Personal Data Protection Practice Group at Lee and Li. Since the *Personal Data Protection Act* was amended in 2010, she has been frequently invited to deliver speeches on the compliance of new *Personal Data Protection Act* both in Taiwan and overseas and has published numerous articles in local and international publications. She constantly advises clients, mostly multinational companies, on the areas of personal data protection, privacy, data security, cross-border data transfer, telemarketing/e-marketing, sweepstakes, online gaming, and electronic signatures, as well as other e-commerce or internet related matters. Ken-Ying has been nominated as an internet, e-commerce and data protection expert by *Who'sWhoLegal* since 2012. She is also the leader of Lee and Li's Mergers and Acquisitions Practice Group (non-financial sector). She was named a Leading M&A Lawyer by Asialaw in 2013 and 2014 and a Leading Lawyer by *IFLR 1000* in 2014.

*__Rebecca Hsiao__

Associate partner

Lee and Li

Rebecca Hsiao is a key member of the Personal Data Protection Practice Group at Lee and Li and practises in the areas of privacy and consumer protection, antitrust and competition law, mergers and acquisitions, securities, and corporate and investment laws. She has constantly advised clients on the compliance of the personal data protection law and delivered speeches on this topic to various government and non-government clients.