BRYAN CAVE
A Broader Perspective
Bulletin

Data Privacy and Security Team

To: Our Clients and Friends September 2013

South East Asia: Data Protection Update

Europe has had data protection laws in place for over a decade. Such laws regulate how data relating to individuals (such as employees or customers) can be collected, used and transferred. Entities that collect and use the personal data of individuals in Europe are required to inform data subjects about the purposes for which their data is to be used and, subject to certain exceptions, to obtain their consent to such use. There are also prohibitions on the transfer of personal data to countries outside of the European Economic Area (being all of the European Union member states plus Liechtenstein, Norway and Iceland) unless the European Commission has determined that such countries have laws that provide adequate safeguards for the protection of personal data. Currently the only two Asia-Pacific countries on the "white list" are Australia and New Zealand. The US is currently not on this "white list". Penalties for non-compliance have recently been increased to £500,000 in the UK, with the possibility of these being increased to 2% of a company's turnover if the new Data Protection Regulations being proposed are adopted.

A number of countries in Asia have started to adopt similar laws on the protection of personal data. Such laws will have an impact on how companies collect and use data from individuals in Asia and how that data can be transferred out of the jurisdiction from which is collected.

Singapore

Singapore passed its Personal Data Protection Act 2012 ("Singapore PDPA") Act last year, with implementation to take place over the next year in order to give businesses time to put in place measures to ensure compliance with the new Singapore PDPA. Both Singaporean organisations and organisations outside of Singapore that are engaged in data use, collection or disclosure within Singapore will have to comply with the new Singapore PDPA. Subject to certain exemptions, organisations may only collect, use or disclose personal data with the individuals prior knowledge and consent, and after informing the individuals about the purposes for such collection. In addition, the purposes themselves must be reasonable in the circumstances. Like the European Data Protection Directive, all individuals have the right to access data relating to them and to correct it. However, unlike the European Data Protection Directive, there is no separate definition of sensitive personal data, such as information about race, health, religion, sexual orientation, political opinions etc., nor do the main provisions of the Singapore PDPA apply to business contact information.

The provisions on the transfer of data outside of Singapore are similar to those in the European Data Protection Directive, namely that a transfer may only be made to an organisation in a different jurisdiction that provides a standard of protection to such data being transferred which is

comparable to the protections under the Singapore PDPA. It is hoped that similar mechanisms to ensure compliance as those implemented in the European Union will be accepted, such as the use of contractual clauses and binding corporate rules.

All organisations subject to the Singapore PDPA must designate a data protection officer irrespective of size. However, there is no current requirement to register the use of personal data with the data protection authorities.

The Singapore PDPA also introduced a Do Not Call Registry. This allows individuals to register their Singapore telephone numbers in order to opt out of receiving marketing telephone calls, SMS, MMS or faxes from organisations. The onus is then on organisations to check with the DNC Registry before sending messages to individuals.

Penalties for non-compliance include fines of up to S$1m (US$790K) and/or imprisonment for up to 3 years. In addition, individuals have the right to bring a civil claim against an non-compliant data organisation.

Malaysia

Malaysia's Personal Data Protection Act 2010 ("Malaysian PDPA") was intended to come into operation on 16 August 2013 with users of data having only 3 months to put in place measures to ensure compliance with the first phase of implementation of the Malaysian PDPA and most, if not all, users of data having to register with the Personal Data Protection Department by 15 November 2013. However, the Malaysian PDPA will not require data protection officers to be appointed by company's using data.

The Malaysian PDPA has a lot of a similarities with the European Data Protection Directive. It applies to persons established in Malaysia and to persons who are not established in Malaysia but who use equipment in Malaysia for processing personal information. It also does not apply to personal data processed outside of Malaysia, unless that data will be further processed in Malaysia. The Malaysian PDPA also distinguishes between personal data and sensitive personal data, with more stringent requirements applying to the latter.

The Malaysian PDPA requires users of data to comply with a number of principles, the General Principle, the justification for the processing, such as consent; the Notice and Choice Principle, the right to be informed about the purposes for the processing; the Disclosure Principle, no disclosure except in connection with the purpose; the Security Principle, the obligation to take practical steps to protect data; Retention Principle, not to keep the data for longer than necessary; Data Integrity Principle, ensure that data is accurate and up to date; and the Access Principle, an individuals right to have access to his or her data.

There are also provisions on transfers of data out of Malaysia which again are similar to those in the European Data Protection Directive. Data users can transfer data to a place specified by the Minister for Information, Culture and Communications, or in accordance with one of the exemptions, e.g. with the individual's consent or for the performance of a contract.

A violation of the Malaysian PDPA may attract criminal liability giving rise to fines or imprisonment.

The Philippines

The Philippines enacted the Data Privacy Act 2012 ("Philippines DPA") last year and like the Malaysian Act, it was also influenced by the European Data Protection Directive

The Philippines DPA applies to personal data and sensitive personal data. It applies not only to persons established in the Philippines, but also to persons established outside the Philippines who are engaged in activities relating to the personal information of a citizen or resident of the Philippines. However, the Philippines DPA does not apply in respect of information collected from residents of foreign jurisdictions. This is surprising because although the Philippines DPA is similar to the European Data Protection Directive the European Commission is unlikely to treat the Philippines as a country ensuring adequate safeguards for personal data, if it does not apply to data collected from residents of foreign jurisdictions.

Whilst the Philippines has created a National Privacy Commission, there is no system of mandatory registration, but organizations will have to appoint a data protection officer who shall be accountable for the organization's compliance with the Philippines DPA.

Similar to the European Data Protection Directive, the Philippines DPA encompasses principles of transparency, legitimate purpose and proportionality. These principles state that personal information must be collected for specified and legitimate purposes, processed lawfully and fairly, be accurate, not excessive and only retained for as long as necessary. The principle of lawful and fair processing requires that personal data can only be processed if certain conditions are satisfied, such as obtaining the consent of the data subject, or if the processing is in connection with the fulfilment of a contract. More stringent conditions exist for the processing of sensitive personal data.

Unusually, there is no prohibition on the transfer of personal data overseas, but organizations that receive data about a citizen or resident of the Philippines may become subject to the Philippines DPA as a result. Furthermore, if an organization transfers data to a data processor (being someone who processes data on behalf of an organisation) whether in the Philippines or overseas, the organization remains responsible for ensuring that proper safeguards are in place, so it is likely that data processor agreements will need to be entered into at least in respect of cross-border transfers of data to processors.

Penalties for a breach include imprisonment of between 1 and 7 years for serious breaches and fines of up to PhP 5 million (US$115,000).

Taiwan

Taiwan passed the Personal Information Protection Act ("Taiwanese PIPA") in April 2010 but it did not come into force until October 2012 due to the controversial nature of some of the provisions which still remain under review. It was enacted as an amendment to the Computer-Processed Personal Data Protection Act ("CPPDPA") which covered the collection, processing and use or personal data by certain regulated entities.

The scope of the new act is broader that the CPPDPA, in that it is no longer limited to computer processed data and it will apply to all individuals, legal entities and enterprises that collect

personal data. The Taiwanese PIPA applies to personal data and sensitive personal data. (although the provisions on sensitive personal data proved to be so controversial that there has been a delay in their implementation). There are no registration requirements and a data processor does not have to nominate a data protection officer who must ensure compliance with the Taiwanese PIPA.

Under the Taiwanese PIPA, a data subject must be provided with adequate notice before a data controller first collects personal data from it, such notice must include the purposes of the collection, how the data will be used and the data subject's right of access. In addition, if the data controller receives information about a data subject indirectly, it must notify the data subject of the sources of such personal data.

The collection and processing of data must be for specific purposes and comply with certain requirements, such as be collected pursuant to a contract, or with the written consent of the data subject.

With respect to cross-border transfers of data, these can be prohibited by the competent authority in certain circumstances, including if the country to which the data is being transmitted does not have sound legal protection for personal data.

Penalties for breach can include criminal sanctions, administrative fines and civil action.

South Korea

South Korea is reported to have the most stringent laws on data protection in Asia. The Personal Information Protection Act ("South Korean PIPA") came into force in March 2012 and contains the concept of both personal data and sensitive personal data. Save for a few limited exemptions, data can only be collected and processed with prior consent, and only after the data subject has been informed of the purposes of such collection and use. A separate consent must be obtained for processing sensitive personal data, and certain processing activities such as transfers abroad or business transfers. The data collected must be proportionate to the purposes and the data must be safeguarded from unauthorised access.

Organisations must register with the Minister of Public Administration and Security and appoint a data protection officer.

Although these principles are similar to the provisions of other data protection acts, the South Korean PIPA goes further than most data protection acts in that it explicitly states that only the minimum collection of data necessary for the purposes is allowed and a data processor cannot refuse to provide goods or services to a data subject because they do not consent to the collection of data exceeding this minimum requirement. The South Korean PIPA even goes so far as to require processors to make efforts to process data in anonymity if possible.

These provisions are reinforced by the extensive rights given to data subjects. Not only do they have the right to access their data and request corrections to be made, but they can also suspend the use of their data and withdraw their consent to processing of their data in the context of a business transfer. Most significantly, if a data processor is accused of non-compliance by an

aggrieved party, the onus of proving that the data processor has complied is on the data processor itself, rather than the data subject bringing the compliant.

Therefore data processors in South Korea will have to ensure that they have the appropriate records in place to show full compliance with the South Korean PIPA. This will not only mean complete records of consents for all processing, but also assessments on whether personal data is needed to achieve the purposes for which it is being obtained.

Penalties for non-compliance include imprisonment and fines of up to 100 million won (US$92,000).

Conclusion

The Asia Pacific Economic Cooperation ("APEC") Privacy Framework, is a framework which has been endorsed by the APEC economies as a tool for encouraging the development of appropriate data protection policies and laws. The framework is consistent with the privacy principles of the Organisation for Economic Co-operation and Development ("OECD"), which were also used as the basis for the European Data Protection Directive. Therefore, it is no surprise that the Asian data protection acts bear such similarities to the European Data Protection Directive, as all of the countries listed above (except Taiwan) are APEC members.

As stated above, only Australia and New Zealand have been deemed by the European Commission to have adequate safeguards in place for the transfer of data from European member states. However, depending on how well the new data protection laws coming into force in Asia are implemented and enforced, we may see more Asian countries being added to the "white list" making the flow of data from Europe to Asia far easier.

With respect to compliance with these new law, the experience of implementing data protection policies and procedures in Europe will benefit organisations when seeking to comply with the new data protection laws in Asia. However, it will be important for organisations to continually conduct reviews of their data protection policies to ensure that they comply with local legislation, for example some require the names of third party data processors to be provided, or details of the organisation from which information was obtained by them. In some jurisdictions organisations will also have to check that the manner in which they obtain data is legitimate in that jurisdiction, or otherwise obtain consent. Organisations may also have to register in certain countries and to appoint an appropriate individual to act as a data protection officer.

This bulletin provides only a brief summary of some of the laws that have been implemented recently. Other countries are also looking to adopt their own specific data protection laws (Thailand currently has a personal data protection bill under review) whilst certain countries that have existing laws in place are reviewing and revising them to keep up with global developments in privacy protection, for example the People's Republic of China recently passed a Resolution Relating to Strengthening the Protection of Information on the Internet and Hong Kong recently amended their data privacy laws to prevent companies from using personal data in direct marketing without getting consent from the people being targeted.

For more information on this subject, please contact:

Gupinder Assi
Singapore
Direct Dial: +65 6403 6391
ggassi@bryancave.com

Bryan Cave's alerts/bulletins/briefings are available online at www.bryancave.com/bulletins.