New tough privacy regime in the Philippines Data Privacy Act signed into law

Intellectual Property and Technology News

17 OCT 2012
By: Arthur Cheuk

15 August 2012 marked the birth of the Data Privacy Act of 2012 ('Act') – the Philippines' first ever consolidated data privacy legislation, which was significantly influenced by Directive 95/46/EC of the European Union and the Asia Pacific Economic Cooperation ('APEC') Information Privacy Framework. The introduction of the Act follows a series of developments in the expansion of data privacy laws in the Asia Pacific region and adds to an increasingly complex data privacy environment, particularly for organisations using business process outsourcing ('BPO') services based in the region.

The Act aims to substantially raise the profile of the Philippines in the data privacy (and business in the data processing) sphere by mandating that all personal information controllers ('Controller'), being persons who control the collection, holding, processing or use of the personal information of others (defined in the Act as 'Data Subjects'), comply with a raft of requirements before any such collecting, holding, processing or use may take place.

In the Philippines it is hoped that the Act will allay concerns over the security of personal information handled by employees of BPO companies based in the Philippines, which in turn will attract more investors in the information technology and BPO industry in the Philippines. The Philippines Business Processing Association believes that the Act will facilitate the IT – BPO industry expanding from call centers to areas that involve handling sensitive personal data such as in the health care and human resources areas, with projections of revenue in the industry increasing from USD 9 billion in 2011 to USD 25 billion by 2016.

Of particular note: The Act is one of the toughest data privacy legislations in the region, in terms of sanctions imposed on offenders. The Act introduces:

- Fines and prison sentences for first time breaches of the Act
- Ongoing liability of Controllers for personal information sent offshore/provided to third party processors
- Significant rights of Data Subjects, and
- The fact that companies that breach the Act may be prevented from processing personal information and individual foreigners who breach the Act will be deported.

What the act applies to

The Act regulates the 'processing' of personal information, which is broadly defined to include any operation performed on the information, such as collection, organisation, modification, retrieval, consultation, use, blocking, erasure and destruction. 'Personal information' is defined, as in many other privacy regimes of the region, as any

information from which the identity of the Data Subject is apparent or can be reasonably and directly ascertained or that, when put together with other information, will identify the Data Subject.

In accordance with its EU-influenced heritage and similar to the Australian privacy regime, the Act introduces the concept of 'sensitive personal information', a class of personal information which (due to its particular sensitivity) is subject to more stringent requirements for processing. Examples of such information include political affiliations, race, ethnic origin, marital status, age, sexual life, health information (including genetic information), criminal record, social security numbers and tax returns.

The Act also applies to Controllers and entities which are not established in the Philippines if

- The personal information is about citizens or residents of the Philippines
- The entity has a 'Philippines link', examples of which include contracts entered into the Philippines, or where a branch, agency or subsidiary of the entity is established in the Philippines, and
- The entity has "other links" with the Philippines, such as carrying on business there or if the personal information was collected or held in the Philippines.

However, the Act does not apply to personal information which is originally collected from non-Philippine residents in accordance with the applicable foreign law, even if processed in the Philippines. This means that outsourced processing in the Philippines is exempt where data has been collected overseas, in an attempt to protect the Philippines IT – BPO industry. In actual fact, as the applicable foreign laws will continue to apply, outsourcing to the Philippines will remain cumbersome for the EU, Australia and other countries with data export restrictions.

A new national regulator for privacy

An independent privacy regulator, (the National Privacy Commission ('NPC')), will be established to administer and implement the Act. Attached to the Department of Information and Communications Technology and headed by a Privacy Commissioner, the NPC will be responsible for the enforcement and administration of the Act. The NPC's powers include handling privacy-related complaints, conducting investigations, issuing orders for compliance and issuing temporary or permanent bans on data processing by named Controllers.

General principles for the processing of personal information

Similar to many data privacy regimes in the region and globally, the Act sets out general data privacy principles ('Principles') by which all Controllers must abide. In brief, the Principles stipulate that personal information must be:

- Collected for specified and legitimate purposes, which must be declared to the Data Subject before collection (or as soon as reasonably practicable after collection)
- Processed (ie used) fairly and lawfully
- Accurate and not excessive for the purposes for which it is collected and processed
- Retained only for as long as necessary for the stated purposes, and
- Anonymised or de-identified as soon as possible, subject to limited exceptions.

Conditions for the lawful processing of personal information

In addition to complying with the Principles, all Controllers must ensure that any processing of personal information (ie not sensitive personal information) must only take place if at least one of the following conditions apply:

- The Data Subject has given his/her consent, which must be evidenced by written, electronic or recorded means
- The processing is necessary to fulfil a contract with the Data Subject or to fulfil the Data Subject's requests prior to entering into the contract
- The processing is necessary for compliance with the legal obligations of the Controller
- The processing is necessary to protect the vital interests of the Data Subject (such as his/her life or health)
- The processing is necessary to respond to national emergencies, or
- The processing is necessary for the purposes of the legitimate interests of the Controller or third party recipients of the personal information, subject to the fundamental rights of the Data Subjects.

The processing of sensitive personal information is generally prohibited under the Act unless:

- The Data Subject has given his/her consent (though not expressly stated, we expect in writing or by electronic or

recorded means)
- The processing is expressly permitted by law
- The processing is necessary to protect the life or health of a person or persons or is necessary for the purposes of medical treatment, or
- The processing is necessary to achieve the lawful and non-commercial objectives of public organisations, subject to the Data Subject's consent, or
- The processing concerns such personal information as is necessary to protect a person's lawful rights and interests in legal proceedings.

Notification required prior to collection

Following the EU and numerous regional privacy models, the Controller must generally notify the Data Subjects of the particulars of the processing (ie proposed uses of the information) before collecting their personal information and entering it into their processing systems (or as soon as practically possible thereafter). The particulars that the Data Subject must be notified of are:

- A description of the personal information to be collected/entered into the system
- The purposes of the processing (ie uses of the information)
- Scope and method of the processing
- Possible recipients or classes of recipients to whom the personal information may be disclosed
- Methods by which the personal information may be accessed automatically
- Identity and contact details of the Controller, and
- The Data Subject's rights to access and correct their personal information, as well as his/her right to make complaints to the NPC.

However, notification is not required under certain limited circumstances, including where the processing is for 'obvious purposes'. Examples of such 'obvious purposes' include circumstances where the processing is necessary for the performance of a contract entered into by the Data Subject, in the employment relationship between the Controller and the Data Subject and where the collection and processing are done as a result of a legal obligation.

Transfer of personal information and subcontracting

Unlike some regional jurisdictions, the Act does not prohibit or restrict the overseas transfer of personal information. However, where personal information is sent to a third party for processing, the Controller remains accountable for complying with the Act, irrespective of whether the third party processor is located in the Philippines or overseas.

To the extent that personal information is transferred to third parties for processing, Controllers must impose on third party processors the same security obligations as imposed on the Controller under the Act (see under the heading 'Security Measures' below).

Rights of data subjects

Data Subjects have a number of rights under the Act, many of which could potentially translate to significant administrative costs for Controllers. For example, Data Subjects have the right to demand from the Controller reasonable access to a wide variety of information, including the following:

- His/her personal information which has been processed
- Sources from which the personal information has been obtained
- Names and addresses of the recipients to whom the personal information has been disclosed
- The manner by which the personal information was processed
- Reasons for disclosing the personal information
- Information on any automated processes by which the personal information may be used as the sole basis for decisions which will affect the Data Subject, and
- The date of last access or modification of the personal information.

This list of information which Data Subjects are entitled to request access to goes beyond the access and correction rights found in the data protection laws of many regional jurisdictions. In particular, the sources of

personal information, names and addresses of the recipients and information on automated processes will impose on Controllers a heavy burden of keeping detailed records on their data handling practices. In addition, Data Subjects have the right to dispute inaccuracies in their personal information, request the erasure or destruction of any of their personal information which is found inaccurate or used or collected without their authorisation.

To the extent that a Data Subject suffers damage as a result of any inaccurate information or unauthorised use of his/her personal information, the Controller/organisation is required by the Act to indemnify him/her against all such damage. This places considerable pressure on Controllers to ensure that the personal information they collect and use is collected and processed in accordance with the Act, the Principles and the consent from the Data Subject, as well as kept accurate, up to date and secured.

Security measures

All Controllers must implement reasonable and appropriate organisational, physical and technical measures to protect the personal information in their care, particularly against 'natural dangers' (such as accidental loss or destruction) and 'human dangers' (such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination).

What measures are appropriate will depend on a number of factors including the risks involved in the processing, size of the Controller's organisation, complexity of its operations, current data privacy best practices (implying that Controllers must be kept abreast of developments in the data privacy sphere) and the costs of implementing the measures. Subject to further guidance from the NPC, the Act stipulates specific measures which Controllers must implement, such as computer network safeguards, security policies for processing, processes for identifying and assessing reasonably foreseeable vulnerabilities in computer networks, breach-correction measures and regular monitoring for security breaches.

Breach notification

In the event of a security breach involving sensitive personal information or personal information that may be used to enable identity fraud (if the Controller or the NPC believes is likely to give rise to a real risk of harm to the affected Data Subjects), Controllers are required to notify both the NPC and the affected Data Subjects. Non-compliance with this requirement may result in criminal prosecution and is punishable by imprisonment of between 18 months and 5 years and fines between PHP 500,000 and PHP 1 million (approximately USD 12,000 to USD 24,000).

No second chances (severe sanctions)

Non-compliance with the Act generally can result in serious ramifications. Unlike some regional jurisdictions such as Hong Kong and Australia where non-compliance with most provisions only results in enforcement notices (the breach of which in Hong Kong is then a criminal offence), the Act offers no second chances and breaches of the Act are automatic offences. Depending on the nature of the breach, Controllers may be penalised by imprisonment for between 3 and 6 years and fines between PHP 500,000 and PHP 4 million (approximately USD 12,000 to USD 96,000) for individual breaches.

Multiple breaches of the Act may also be penalised by imprisonment for between 3 and 6 years and fines of between PHP 1 million and PHP 5 million (approximately USD 24,000 to USD 120,000). Furthermore, any breaches where 100 or more persons are harmed or affected will be subject to the maximum penalties.

Any company that is found to have breached the Act (such as to constitute an offence) may also have its right to process personal information revoked. In addition, of note for foreign individuals dealing with personal information in the Philippines, if the person who breaches the Act is an alien he/she shall be deported from the Philippines without further proceedings after serving any prison term and/or paying any penalties levied.

Getting your business ready: what you need to do now!

The NPC will provide further guidance on the Act by promulgating implementing rules and regulations ('IRR'). To allow existing businesses to come to grips with the new legislation there is a transitory period of one year, which will begin to run from the date the IRR come into effect. New businesses will not get the benefit of the transition period.

However, even if the transition period is applicable, given the level of organisational and technical compliance the Act requires from Controllers and the wide scope of the rights given to Data Subjects, a year for transition seems a very short time. Time is therefore of the essence for organisations to take active measures now to prepare their data collection, handling and processing/use practices for compliance with the Act. Examples of key steps to take now include:

- Reviewing existing data protection and security practices
- Updating data collection / customer take-on documentation
- Reviewing processor contracts, and
- Developing internal data privacy guidelines protocols.

Of course, we are happy to assist you to prepare for this and with any of your regional or global data privacy requirements.