Publication: The Business Times, p 24
Date: 13 September 2017
Headline: Honing personal data protection

Honing personal data protection

Proposed changes to the law take into consideration the interests of individuals and organisations, and this includes consumers and businesses. BY WARREN B CHIK

THERE are evolving modes of collection and legitimate uses of personal data that should be considered in order to ensure that Singapore's data protection laws are practical and up to date. That is the message coming from the Personal Data Protection Commission (PDPC) in proposed amendments to the Personal Data Protection Act (PDPA).

The proposed changes take into consideration the interests of individuals and organisations, and this includes consumers and businesses. This is in line with the objective of the Act, which sets a reasonable standard for compliance by the latter.

The first of two main proposed amendments will clearly be beneficial to businesses.

They involve the introduction of two alternatives for businesses from having to seek consent for the collection, use and disclosure of personal data from consumers, which is currently the main requirement relating to the management of personal data and that can be quite onerous.

The first alternative is to allow for a notice ("notification of purpose") to suffice in lieu of having to seek consent from every consumer whose personal data they intend to collect, use or share. The other option, if available, is to do so under an exception for a "legal or business purpose".

There is already a provision for deemed consent and a laundry list of exceptions under the current PDPA that is useful for businesses. However, the proposed changes can better accommodate and encourage business innovation while adhering to the main principles of data protection. It will allow for more cases of data handling without having to seek consent, which can be a barrier to better service offerings.

These alternatives are less burdensome and flexible enough to cover new situations or circumstances without the need for legislative amendment (which is currently the case with the listed exceptions approach).

To ensure that individuals' interests are not adversely affected, the PDPC has also proposed some conditions for businesses intending to rely on the proposed alternatives to the consent requirement. These reinforce the "reasonableness test", which is to balance the interests of both sides.

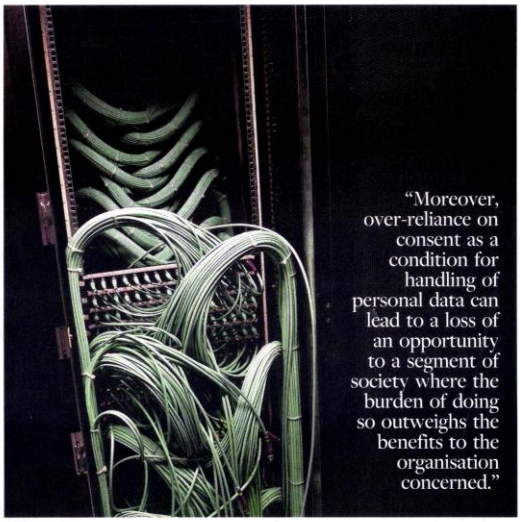
The proposed criteria for the notice-only option is: First, that it is impractical for the organisation concerned to seek consent; and second, the collection, use or disclosure of the personal data is not expected to adversely impact the individuals concerned.

For example, a business that does not have the contact information of its customers but wishes to use their personal data for a new purpose of conducting business analytics to develop new products and services can fulfil these criteria. Another example is where an organisation deploys sensors or drones with recording devices to collect high volumes of personal data of a large number of individuals (which makes it impractical to seek consent from them).

The criteria for the "legal or business purpose" exception is: First, it must be shown that it is not desirable or appropriate to obtain consent under the circumstances; and second, the public or societal benefits outweigh any adverse impact or risk to the individuals concerned.

An example of when this exception can apply is where a group of organisations in a particular industry may wish to share and analyse the personal data of their customers to investigate, identify and detect fraudulent activities (in which case, seeking individual consent may defeat that purpose).

The use of these alternatives also addresses the privacy concerns of individuals that would prefer to be less bothered with repeated and voluminous requests for their personal data. At the same time, they are not meant to allow businesses to avoid seeking individuals' consent for marketing where it is reasonable to do so.



"Moreover, over-reliance on consent as a condition for handling of personal data can lead to a loss of an opportunity to a segment of society where the burden of doing so outweighs the benefits to the organisation concerned."

Moreover, over-reliance on consent as a condition for handling of personal data can lead to a loss of an opportunity to a segment of society where the burden of doing so outweighs the benefits to the organisation concerned.

For example, it may not be commercially practicable to obtain consent from certain individuals for their personal data – such as due to literacy, age or language barriers – in order for organisations to offer them services that may actually benefit them.

These proposed changes are important for a country developing a data economy, and hoping to tap the infinite possibilities that data analytics allow for the benefit of its society. Empirical data derived from the collection and analysis of personal data by scientists and information system experts can be used to enhance standard of living, quality of life and the delivery of services to consumers. They also provide businesses more effective (and cost or labour efficient) ways to reach out to consumers.

NEITHER NOVEL NOR NEW

It is worth noting that these alternatives to the traditional consent requirement are not novel or new and have, in fact, been tested and implemented in countries with more mature data protection laws such as Australia, New Zealand and Japan (as well as in the European Union).

The suggestion of mandatory data breach reporting is in line with the trend towards security breach reporting generally, such as in national cybersecurity laws, which is also being considered in Singapore. It encourages greater care and accountability by data collectors and users, and it is understandable that organisations will be wary of such measures since it places an additional burden on them on top of the other data protection obligations under the PDPA regime.

However, mandatory reporting may not be onerous, and its benefits outweigh the burden, if looked at from a different perspective. Mandatory reporting is primarily meant to arrest any further breach or a worsening of the situation, which is in line with the protective objective of the PDPA.

At the same time, businesses can take the opportunity to showcase the robust measures that they have in place to prevent and arrest data breaches. This will instil greater consumer confidence in their processes and encourage more transactions.

The breach itself need not be due to a lapse or a breach of the security measures for data protection by an organisation. Even if it is, responsive reporting will be a mitigating factor that the Commissioner will consider when determining the appropriate enforcement action, including whether to mete out a financial penalty, and if so, how much. Current shortcomings in reporting are taken into consideration by the Commissioner in its enforcement decisions.

Moreover, the PDPC is suggesting some criteria for mandatory reporting to limit it to cases that are reasonable for such measures to be taken. The current permutation includes data breaches that have a risk of impact or harm to affected individuals or where the scale of the breach is significant.

The criteria were proposed by PDPC so that organisations would not be overly burdened. The reporting requirement also allows individuals to take steps to protect themselves and the PDPC to address systemic issues.

The requirement for data intermediaries to immediately notify the primary organisation can also benefit the latter as they can then take necessary measures as soon as possible. For organisations, the notification timeframe proposed is not immediate and they are only required to notify affected individuals "as soon as practicable". Organisations that encrypt their data as a form of best practice may benefit from the technological protection exemption from the breach reporting requirement.

Finally, any requirement for reporting under the PDPA is intended to dovetail with that found in other sectoral laws or regulations so that it will not require additional resources or effort to report the breach to the PDPC.

The PDPC remains open to feedback on the proposal until Sept 21. Hence, any organisation with concerns or suggestions can still submit their responses by that date.

The writer is an associate professor at the Singapore Management University's School of Law