WITH PERSONAL DATA COMES GREAT RESPONSIBILITY

With the rise of the digital marketplace, Singapore businesses should be mindful in handling their online transactions and interactions with customers and their personal data

BY ***CHESTER TOH*** *&* ***TAN JEN LEE***

ILLUSTRATION: ISTOCK.COM/IRINA_STRELNIKOVA

TWO words were at the tip of everyone's tongue last year: data protection. With the flurry of companies scrambling to comply with the EU's General Data Protection Regulation (GDPR) in May and the aftermath of the SingHealth cyber attack that compromised the data of about 1.5 million patients, including the personal data and medical information of Singapore Prime Minister Lee Hsien Loong, 2018 was arguably the wake-up call that most Internet users needed to start questioning the whereabouts of their personal data and what it was really used for.

According to a joint study by Google and Temasek in November 2018, South-east Asia's Internet economy reached an inflection point last year; and Internet industries – including e-commerce, online travel and ride hailing – are expected to hit a value of US$240 billion by 2025.

With the rise of the digital marketplace, how should Singapore businesses handle such online transactions and its interactions with customers and their personal data?

THINK BEFORE YOU COLLECT

SMEs must familiarise themselves with the obligations and requirements under the Personal Data Protection Act (PDPA) in Singapore. There are broadly nine obligations imposed by the PDPA, out of which three relate to consent, purpose and notification.

In this regard, it is not enough for organisations to simply obtain consent from a data subject. The data subject must first be notified of the purposes for which his personal data is collected, used or disclosed for his consent to be valid. The concept of reasonableness is also key to the PDPA, which means that companies can only collect data that would be considered appropriate to a reasonable person in the circumstances.

As much as SMEs are tempted to provide a generic notification to collect personal data for any and all purposes, this would not meet the mark in complying with the PDPA.

Fortunately, the Personal Data Protection Commission (PDPC) is cognisant of the practical difficulties that organisations face in obtaining consent from consumers for every purpose against the need to provide a seamless range of services that leverage on the consumers' Internet of Things (IOT) devices.

Thankfully, the PDPC has since expressed its intention to recognise a "deemed consent by notification" approach in limited instances. An individual can be deemed to have given valid consent if he fails to opt out within a reasonable time from an organisation's collection, use or disclosure of his personal data after being notified of the relevant purposes.

This approach can only be relied on if the collection, use or disclosure of personal data is not for direct marketing purposes or expected to have an adverse impact on the individual. Otherwise, small and medium-sized enterprises (SMEs) are always recommended to obtain express, written consent. We expect the PDPC to issue updated guidelines addressing the changes to the consent framework over the course of this year.

COLLECT AT YOUR OWN RISK

Another important clarification came when the

PDPC issued guidelines to enhance consumer protection against indiscriminate and unjustified collection, use and disclosure of NRIC, FIN, Work Permit and passport numbers.

From Sept 1 this year, organisations will not be allowed to collect, use or disclose such unique and sensitive identifiers unless it is required under law or is necessary to accurately establish or verify the identities of the individuals to a high degree of fidelity.

The latter includes instances involving significant safety or security risk, or a possibility of significant impact or harm to an individual or the organisation in industries such as health care, finance or insurance.

With this development, SMEs should reassess the rationale and purpose behind any existing collection of NRIC, FIN, Work Permit and passport numbers (or retention of physical copies), as it will need to provide convincing justifications when requested either by the individual or the PDPC.

Otherwise, it is recommended that alternative identifiers are used. These may include partial NRIC numbers (eg XXXX1234A), organisation-issued QR codes or user-generated IDs or user names.

IDENTIFY YOUR DPO

The PDPA also regulates how a company deals with collected personal data and the level of transparency that should be preserved in the relationship between the organisation and the individual.

All organisations – including SMEs, sole proprietors and non-profit organisations – should be mindful that the PDPA requires the appointment of a data protection officer (DPO) responsible for managing personal data information flows and compliance with the PDPA.

The DPO plays a central role in dealing with access and correction requests received from members of the public, and must provide a response to an access or correction request within 30 days. Contact information of the DPO, including a business telephone number and e-mail, must also be made available to members of the public.

These timeframes imposed by the PDPA mean that all organisations, large and small, are expected to have clear systems and internal procedures in place to efficiently handle requests from data subjects.

Although the PDPA does not prohibit a DPO from wearing multiple hats in an organisation, the DPO must be familiar with the PDPA and not simply act as a figurehead. It is no surprise that SMEs find themselves stretched to allocate the right amount of human and financial resources to meet the compliance costs of personal data protection.

In light of the specific carve-out under the GDPR requiring SMEs to appoint a DPO only if its core activity deals with processing of sensitive data or regular and systematic monitoring of individuals that can pose a threat to individual rights and freedoms, it remains to be seen whether the PDPC will consider a similar approach for SMEs here.

MANDATORY BREACH NOTIFICATION

Under the PDPA, organisations are expected to make reasonable security arrangements to protect personal data in their possession or under their control. Unfortunately, with the prevalence of IOT devices, a 2018 *Symantec Internet Security Threat Report* has showed that we are exposed to at least 600,000 Web attacks each day. This means that it is often not a question of "if" but "when" an organisation will be faced with a data breach.

Planning is therefore critical, and it is important for every SME to develop and implement a data breach management and response plan with proper notification procedures. Although it is not currently a requirement under the PDPA, the PDPC has recently proposed that mandatory data breach notification requirements be introduced in Singapore in line with international practices.

The PDPC indicated that breaches which are likely to result in significant harm or impact will require notifications to both affected individuals as well as the PDPC, while large scale breach incidences require a notification to the PDPC.

Having considered public and industry feedback on the timeframes for such notifications, the PDPC intends to allow organisations a 30-day assessment period from the day that it becomes aware of a suspected breach, to assess the eligibility of the breach for notification. Once a breach is investigated and deemed eligible for reporting, organisations will have up to 72 hours to notify the PDPC of the breach.

With this new requirement, SMEs are advised to get their ducks in a row so as to avoid a last-minute scramble finding the right personnel and consultants who can advise on the data breach. This will be even more crucial for companies active in multiple countries, as seen from the crisis at Cathay Pacific over a global data breach that led to investigations from 27 regulators from 15 jurisdictions.

THE TRUE COST OF NON-COMPLIANCE

The trend of increased regulation and stricter enforcement regarding personal data protection are showing no signs of slowing down. In the wake of the major SingHealth cyber attack, the PDPC showed no mercy to the organisations involved with the imposition of a combined penalty of S$1 million – the highest ever financial penalty imposed by the PDPA.

Penalties aside, SMEs should also be aware of the intangible losses which can sometimes prove costlier than the financial penalties. These may include reputational damage, diminished goodwill and trust among consumers and loss of future business.

According to the IBM Security-sponsored Ponemon Institute's 2018 *Cost of a Data Breach* study, the average cost of a data breach globally is about US$3.84 million, with all cost factors considered. This is a figure that is rising and expected to rise this year with the proliferation of advanced hacking technologies and mega data breaches. Now, more than ever, is the time for SMEs to step up and regularly ensure that their systems and protections dealing with any personal data are all in place. ■

Chester Toh is a partner and Tan Jen Lee is a senior associate at Rajah & Tann Singapore LLP

ILLUSTRATION: FREEPIK