Lessons from PDPA Enforcement Decisions: Consent Obligation

The Consent Obligation is one of the key data protection obligations in the Singapore Personal Data Protection Act (PDPA).

While organisations may generally be aware of the need to obtain consent when collecting personal data from individuals, it is easy at times to neglect the need to ensure that the personal data is used or disclosed only for the purposes which consent was given.

In 2016, four organisations were found to have breached the Consent Obligation of the PDPA. Among them was a tuition agency which had published the NRIC numbers and photographs of tutors on its website when they had not consented to the disclosure of such information, and a property agent who revealed personal data collected for a tenancy agreement to a third party without consent.

These cases help shed light on one of the more common personal data protection failings among organisations here. They also serve to provide useful reminders of the key steps that organisations should take to comply with the Consent Obligation of the PDPA.

Practices and Processes Matter

In April last year, a tuition agency was issued a warning for publishing the images and NRICs of some of its tutors without their consent. Despite maintaining in its privacy policy that the personal data of its tutors will not be shared with third parties, the agency had published the photographs of the tutors and also unwittingly disclosed the NRIC numbers as these were used in the naming of its tutors' images that were uploaded onto the agency's website.

Such an oversight can occur in any organisation when they do not pay heed to corporate policies, even if the right policies are in place. Whether or not it is a genuine mistake, stakeholders' trust

can erode and depending on the severity of the breach of the PDPA, a financial penalty may be imposed on the organisation by the Personal Data Protection Commission (PDPC) in a suitable case.

Breaches of the PDPA, as in the case of the tuition agency can be avoided if organisations take greater care in ensuring consent was given each time before personal data of their customers is collected, used or disclosed. Regular audits to ensure that business and operational practices and processes are aligned with the organisation's personal data protection policies would also go towards preventing unintended breaches of the PDPA.

Repurposing Personal Data Requires Consent

Another case surrounding the Consent Obligation involved a property agent who was fined $500 for disclosing the personal data of his client's tenant and the tenant's wife without their consent.

In this particular case, the property agent had collected personal data from two tenants in order to execute a tenancy agreement. He later provided some of these details to another party and when investigated, argued that he had done so in his personal capacity.

Providing the grounds for its enforcement decision, PDPC pointed out that since the personal data was collected in the course of the real estate work, it was for the property agent's business purpose and not for his personal or domestic purpose. Therefore, a person cannot take personal data collected in his commercial capacity and disclose it in his personal capacity without the relevant consent from the individual or individuals concerned.

Personal Data from Third-Party Sources

Apart from the cases cited, organisations should also be mindful of other potential breaches of the Consent Obligation of the PDPA.

When obtaining personal data from third-party sources, an organisation should exercise due diligence to ensure that consent had been given for the disclosure and use of the personal data to the organisation for its intended purpose.

Take the example of a customer referring her friend to a spa that is running a special promotion. Before recording the personal data of customer's friend, the sales consultant at the spa should ensure that the friend had given her consent to the disclosure of her personal data to the spa for its marketing purposes.

If the friend's consent was not captured in evidential form and the spa intends to send marketing messages to the friend via voice call, text message or fax, the spa consultant must run a check on the DNC registry to ensure that the friend had not opted out of receiving voice, text or fax marketing

messages. If the friend's telephone number(s) was found on the DNC registry, the spa consultant must abide by the DNC rules and not contact the friend for any marketing purposes.

However, the spa consultant may contact the friend, solely to verify whether she had indeed given her consent to allow the spa to share the special promotion with her.

Withdrawal of Consent

Even after consent is given, organisations must allow individuals to withdraw their consent at any time. Using the earlier example, the spa should provide an easy way for the friend (and any customer) to withdraw consent. For example, the spa could, in their marketing SMS to the friend, make available a facility for notifying withdrawal of consent (e.g. "to unsubscribe, reply UNSUB to 9988"). In this regard, organisations should also clearly indicate the scope of withdrawal via such facility to avoid dispute. Otherwise, if the modes of communication that the individual is withdrawing consent from is not made clear, the PDPC would generally consider the withdrawal of consent to apply only to messages sent via that channel. For example, it would typically be reasonable for a retailer to assume that Jane is only unsubscribing from SMS notifications when the retailer who has the consent of Jane to send her marketing messages via voice call and SMS receives a general unsubscribe request from Jane via SMS. On receipt of notice of withdrawal, organisations should also notify the individual of the likely consequences of the withdrawal.

In facilitating any notice to withdraw consent, an organisation should act reasonably and in good faith. When withdrawals are received, organisations should take care to update its database promptly to avoid breaching the PDPA by contacting and upsetting individuals who have withdrawn their consent.

Consent to Seek Consent

Notwithstanding a customer's withdrawal of consent on a particular purpose, organisations may, under certain circumstances, still seek the consent of the individual on the use or disclosure of his personal data in a new transaction.

For example, a Telco must not continue to send promotional updates on a broadband service to a customer after receiving his withdrawal notice. However, a new broadband service was launched some time later and the Telco wishes to inform the customer. Is the Telco allowed to do so? The Telco may do so by seeking fresh consent from the customer at the point of contract renewal. In such instances, the Telco should also take care to comply with the Do-Not-Call provisions if the consent was to be obtained via voice call, SMS or fax.

However, in circumstances where the collection, use or disclosure of personal data is required or authorised under the PDPA or other laws, consent will not be needed.

Conclusion

Through its enforcement actions in these areas and its Advisory Guidelines, PDPC seeks to strike a balance between what organisations can do with personal data and what individuals are entitled to. Ultimately, the goal is to ensure that organisations are able to maintain and benefit from a high level of trust from customers while being able to participate fully in the new data economy.

"Our data protection law places equal emphasis on what data subjects are entitled to and what organisations are obliged to safeguard. While we work to help organisations comply with the PDPA, we are at the same time mindful not to stifle the use of personal data innovatively and productively"

- Mr Yeong Zee Kin,
Deputy Commissioner of the PDPC