Engendering Trust

There is a strong case to be made for organisations to seek consent for the collection, use and disclosure of personal data, beyond the need to comply with the Personal Data Protection Act (PDPA). As one of the key tenets of personal data protection, the consent obligation helps businesses manage the cost and effort involved in collecting, storing and protecting excessive amounts of data. It also enables businesses to make more effective use of the personal data that they have collected.

What Constitutes Personal Data?

Personal data refers to data that can be used to identify an individual. It is common practice for organisations to collect personal data by asking individuals to fill up a form or to key in their details when applying to join a company, registering for a service or programme, arranging for deliveries or carrying out other transactions.

However, personal data can take other forms as well. In the travel industry, for example, photographs taken of people on a tour could also be constituted as personal data. As Ms Janet Chan, Data Protection Officer of Chan Brothers Travel, explained, "When travellers join us for a holiday, our organisation takes group photos, which we will give to all individuals on the same tour so that they can keep to share and reminisce in the future. However, a person's face is also considered as a piece of personal data which cannot be collected unless consent is given."

To address this, Chan Brothers Travel introduced a new clause allowing passengers to alert the travel agency during their booking if they do not want their pictures taken on the tour. This is reiterated during the tour briefing as well as the photo-taking session. "We will also remind the travellers to inform our tour leader if they do not want their photograph to be taken or used by the travel agency," said Ms Chan.

Reasonable Amount, Reasonable Use

Beyond "what" constitutes personal data, businesses also need to think about "how much" personal data they need to collect, and under what circumstances they will need to seek consent for its use. An important aspect to consider is not to "over-collect", as holding

excessive personal data will also increase the risks and efforts required to protect it. To minimise the amount of personal data that an organisation has to protect, organisations should develop policies and processes to regularly review if the personal data is still required and stipulate a retention period for such data. Personal data that is no longer required should be properly disposed of.

The PDPA allows for the collection of personal data that is reasonable for an organisation's business use. For example, an online store would need to collect data such as the customer's address and contact details to deliver its products, while an employer would need to know its employees' bank account details in order to bank in their salaries.

At Quality Hotel Marlow, the front office is usually where personal data is collected, as guests are required to furnish their personal details to facilitate the check-in/out process. "We only collect data that are imperative for the check-in/check-out process," said Ms Mayvin Loo, marketing communications executive and DPO for the hotel. "For example, passport number, credit card details and full name are mandatory. Other personal details such as employment status and education level are not required and hence not collected."

There are, however, instances of organisations wanting to collect personal data beyond the scope of "reasonableness". An example would be organisations making the use of personal data a requirement for the provision of goods and services.

In its Advisory Guidelines on Requiring Consent for Marketing Purposes (May 2015), the Personal Data Protection Commission (PDPC) cites scenarios where businesses cannot refuse to provide a service to the customer on grounds that the customer has not given consent for the use or disclosure of their data for particular purposes. For example:

- An education service provider requiring students to provide their name, photograph and examination scores for use in its publicity materials.
- A car cleaning service provider requiring its customers to consent to the sharing of their personal details with third-party marketing agencies.

In these examples, requiring customers to consent to the collection, use and disclosure of personal data for such purposes (or not allowing withdrawal of consent) goes beyond what is "reasonable" to provide the respective service to the individual.

There is no universal criteria for assessing "reasonableness". Organisations will need to contextualise their collection, use and disclosure of personal data within their business operations and needs. Organisations may wish to draw up a personal data inventory map that spells out what personal data is collected and why, who collects it, where it is stored and who it is disclosed to. Having in place appropriate personal data protection policies will help organisations to better identify the set of personal data they would reasonably request for. It will also help organisations become more accountable to their customers and engender trust on their organisations' practices.

"We only collect data that are imperative for the check-in/check-out process."

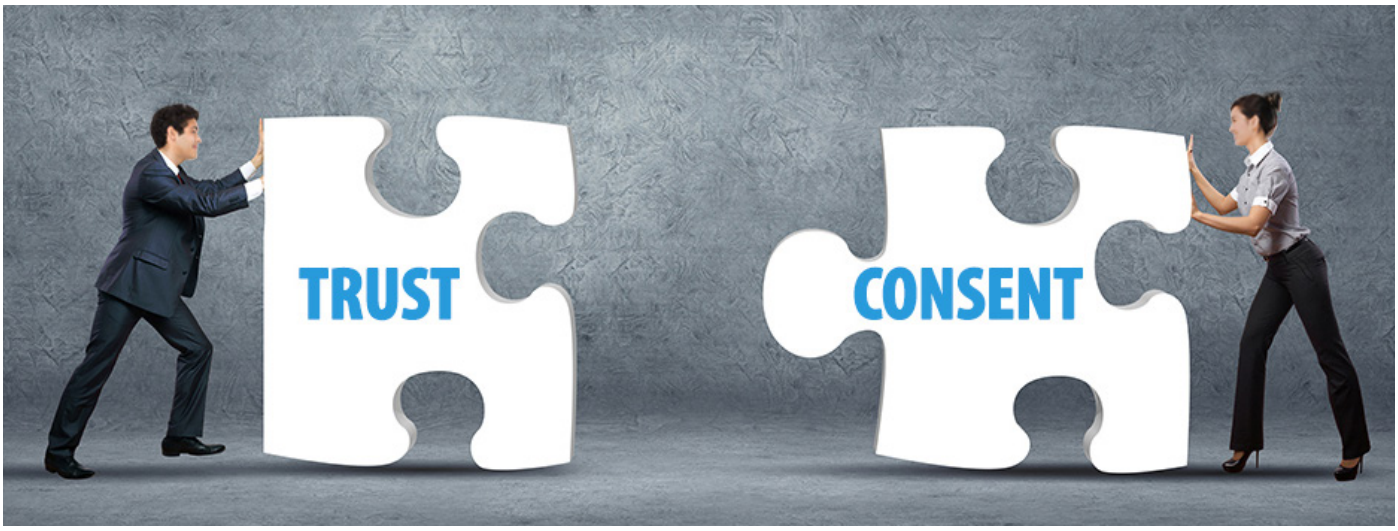
- Ms Mayvin Loo,
Marketing Communications Executive and DPO at Quality Hotel Marlow

Explicit or Deemed Consent

When collecting personal data, organisations also have to inform individuals about the purposes for which the data is being collected, how it will be used or disclosed, and obtain the relevant consent.

Consent may be explicit or deemed. In its most straightforward form, and as good practice, organisations may wish to obtain consent in writing or in a format that can be easily retrieved if there is a need to prove consent in the future.

However, there may be scenarios where the consent is implied or deemed. In its advisory guidelines, the PDPC cites the example of an individual seeking treatment in a medical facility such as a clinic or hospital, and voluntarily



providing his personal data for this purpose. In this case, he would be deemed to have consented to the collection and use of his personal data by the medical facility for purposes related to his treatment.

Another example of deemed consent would be when an organisation holds a private function and wishes to rely on deemed consent to take photographs of the attendees. For the organisation to rely on deemed consent, the organisation will need to take measures to ensure that the attendees are aware that photographs will be taken during the event and how the photographs will be used. The organisation could inform the attendees by indicating in the event invitation, or putting up a notice prominently at the event venue.

The Business Case for Consent

From a business perspective, the consent obligation should not be seen as a hurdle to overcome, but as a catalyst for improving organisational effectiveness, and willingness to provide more personalised services to their customers.

At the very basic level, consent (or the withholding of consent) provides a barometer for gauging individuals' comfort level in sharing different types of data. This can guide organisations in fine-tuning their personal data policies, preventing over-collection of such data and reducing the downstream costs associated with storing, managing and securing the personal data.

From a marketing perspective, consent provides businesses with an effective filter for segmenting their customers and identifying warmer leads. For example, when an individual consents to a car servicing company using his personal data to send him promotions on car-related products, it is a good indication that he would be open to considering these products in his future purchases. This paves the way for the company to sell, cross-sell or upsell products and services that are of value to the customer.

Consent in this case presents a targeted marketing opportunity that benefits both the business and the customer – the customer is on a lookout for particular products or services, and the business may be in a good position to meet these needs.

Respecting the "no" option is just as important. The fact that an individual is asked for his consent indicates that he is empowered to choose whether his personal data can be collected, used or disclosed in the ways spelt out in the terms of consent. And the fact that the organisation acts in accordance to his choice sends a strong signal that the organisation is careful when handling his personal data and offers a more personalised service to its customers. This will, in the long run, help engender trust and strengthen the relationship between the business and its customers.

You can refer to this checklist to help you gauge reasonableness in obtaining consent, review your policies and consider ways to better protect the personal data in your custody.