

**24 September 2013**

## **Factsheet**

# **ADVISORY GUIDELINES ON THE PERSONAL DATA PROTECTION ACT 2012**

## **BACKGROUND**

The Personal Data Protection Act 2012 (the “PDPA”) establishes a new general data protection law in Singapore which governs the collections, use and disclosure of individuals’ personal data by organisations. The PDPA will come into full effect from 2 July 2014.

The Personal Data Protection Commission issued the Advisory Guidelines on Key Concepts and on Selected Topics in September 2013. The Guidelines provide interpretations of the provisions under the PDPA, with a view to help organisations and individuals better understand these provisions. For organisations, the Advisory Guidelines are useful reference points for their review and implementation of data protection processes to comply with the PDPA.

## **ADVISORY GUIDELINES ON KEY CONCEPTS – IN BRIEF**

The Advisory Guidelines on Key Concepts provide interpretations and definitions of important terms used in the PDPA, key obligations of organisations, as well as elaborate on the Data Protection and Do Not Call Provisions in the PDPA.

### **Key Obligations of Organisations**

#### **1. Consent, Purpose Limitation and Notification Obligation**

Organisations must notify individuals clearly of the purposes for which their personal data would be collected, used or disclosed, and obtain consent. Consent is valid only if given for purposes which are reasonable.

**“Photo-taking” generally considered a form of reasonably expected means to collect publicly available personal data without consent**

The PDPA provides for certain exceptions to the obligation to obtain consent. Organisations are able to collect, use and disclose personal data that is publicly available without consent. The term “publicly available” is defined in section 2(1) of the PDPA and refers to *personal data (about an individual) that is generally available to the public, including personal data which can be observed by reasonably expected means at a location or an event at which the individual appears and that is open to the public.*

Personal data is observed by reasonably expected means if the individual whose personal data is being observed ought reasonably to expect that their personal data could be collected in that particular manner at that location or event. The PDPC will take the position that at present; photo-taking would in many circumstances be considered a reasonably expected means of collecting personal data in a public place. However, as good practice, organisations collecting images of individuals in public places should inform individuals of such collection, for example through a notice in the vicinity that such collection is occurring.

## 2. Access and Correction Obligation

Upon request, organisations must provide the individual with his personal data; and inform the individual about how the personal data has been used or disclosed in the past one year.

Organisations need not provide access if exceptions in the Fifth Schedule of the PDPA apply, e.g. if the amount of effort and resources needed to provide access would be unreasonable to the organisation or disproportionate to the individual’s interest.

Organisations must also correct an individual’s personal data upon request, unless satisfied on reasonable grounds that the correction should not be made. Organisations need not correct the personal data if exceptions in the Sixth Schedule of the PDPA apply, e.g., a document related to a prosecution if all proceedings related to the prosecution have not been completed.

### 3. Accuracy Obligation

Organisations should take reasonable steps to verify that the personal data they hold is accurate if they intend to use the personal data to make a decision about the individual, or to disclose the personal data.

### 4. Protection Obligation

Organisations must protect personal data in their possession or under their control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

### 5. Retention Limitation Obligation

Organisations must cease to retain personal data as soon as the purpose for which it was collected is no longer served by the retention, and retention is no longer necessary for legal or business purposes.

### 6. Transfer Limitation Obligation

Organisations must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA.

### 7. Openness Obligation

Organisations must implement the necessary policies and procedures in order to meet their obligations under the PDPA and shall make information about such policies and procedures publicly available.

### Other Rights, Obligations and Uses

Organisations can continue to use personal data collected before the the PDPA fully comes into effect (i.e. 2 July 2014) for **reasonable existing uses**, unless the individual has withdrawn consent. Fresh consent will need to be obtained if the personal data is to be used for other new purposes.

## **Do Not Call Provisions**

Organisations that wish to send specified messages to Singapore telephone numbers after the Do Not Call Provisions come into effect (i.e. 2 January 2014) must either check the Do Not Call (DNC) Registry first to ensure that the numbers have not been registered; or obtain clear and unambiguous consent to do so from the individuals using the Singapore telephone numbers.

Most marketing messages of a commercial nature would fall within the definition of a specified message.

### **Opt-in consent necessary to override DNC registration**

An organisation may send a specified message to a Singapore telephone number registered on the DNC registry if it has obtained “clear and unambiguous consent” in evidential form from the individual to the sending of the message. Clear and unambiguous consent must be given through some form of positive affirmative action. Clear and unambiguous consent is unlikely to be construed to have been obtained from a mere failure to opt out through inaction on the part of the individual.

The Advisory Guidelines provide examples of how organisations may obtain clear and unambiguous consent from individuals for the purposes of telemarketing. One example is replicated here:

#### Example

Sarah fills up an online form. The following clause is directly above the “Submit” button.

I would like to receive information about promotions and offers by:

- a. Phone [ ]
- b. SMS [ ]
- c. Email [ ]
- d. Mail [ ]

Sarah checks the boxes SMS and Email and submits the online form. Sarah would be considered to have given clear and unambiguous consent.

## ADVISORY GUIDELINES FOR SELECTED TOPICS – IN BRIEF

The Advisory Guidelines for Selected Topics elaborates on how the PDPA applies to specific issues and domains.

### **Analytics and Research**

Organisations can obtain consent for research as a separate purpose; or as part of the original purpose for which consent was given.

### **Anonymisation**

The PDPA does not apply to anonymised data. Data would be considered anonymised if the re-identification risk is minimum.

### **Closed-circuit television cameras (“CCTVs”)**

Organisations should provide notification and obtain consent when collecting personal data using CCTVs. The PDPC does not require the placement or content of notifications to reveal the exact location of the CCTVs. Where consent is not required, such as when collecting personal data that is publicly available, organisations may still wish to provide notifications that CCTVs are in operation in the premises as good practice.

### **Employment**

Employers need not seek consent to collect, use or disclose personal data that is publicly available, or for evaluative purposes, e.g. reference checks. Employers should notify employees when using personal data for the purpose of managing the employment relationship.

### **NRIC Numbers**

NRIC numbers are personal data and organisations should comply with the PDPA when collecting, using or disclosing them. As best practice, organisations should avoid over-collecting personal data and consider suitable alternatives for their requirements (e.g. using an individual’s unique membership number and date of birth instead of NRIC number to verify his identity).

*Full details of The Advisory Guidelines can be found on [www.pdpc.gov.sg/personal-data-protection-act/public-consultations](http://www.pdpc.gov.sg/personal-data-protection-act/public-consultations).*

*Organisations that would like to seek clarifications and specific guidance on the Advisory Guidelines could also attend the regular briefings conducted by the PDPA or email PDPC at [info@pdpc.gov.sg](mailto:info@pdpc.gov.sg).*



PERSONAL DATA  
PROTECTION COMMISSION  
S I N G A P O R E

---

**ISSUED BY THE PERSONAL DATA PROTECTION COMMISSION**

---

**About Personal Data Protection Commission**

The Personal Data Protection Commission (PDPC) administers the Personal Data Protection Act 2012 (PDPA) in Singapore, which aims to safeguard individuals' personal data against misuse and promote proper management of personal data in organisations. In addition, the PDPA will enhance Singapore's competitiveness and strengthen our position as a trusted business hub, putting Singapore on par with the growing list of countries with data protection laws. For more information, please visit [www.pdpc.gov.sg](http://www.pdpc.gov.sg).

**For media queries, please contact:**

Ms Jeanne Tan  
Manager, Media Relations  
Personal Data Protection Commission  
c/o Infocomm Development Authority of Singapore (IDA)  
Tel: 6211 1796  
Email: [jeanne\\_tan@ida.gov.sg](mailto:jeanne_tan@ida.gov.sg)