

Personal Data Protection Act (PDPA) Updates

What is new?

June 2016

Personal Data Protection Commissioner (PDPC) has updated its advisory guidelines on 9 June 2016 to provide clarity on two key areas:

1. Providing access to personal data
2. Managing access requests on CCTV footage

A separate guide with sample forms is also published to aid organisations in managing access requests from individuals.

Key updates

Handling access requests

- Organisations should **clearly state the channels** where individuals may submit their access requests. In cases where individuals can retrieve their personal data themselves (e.g. self-help portal), the organisations may inform them on the means to do it.
- The policy and process for handling access requests should take the following into consideration:
 - **Different types of access requests** (e.g. a request made by the individual himself, a request made on behalf of another individual or a request made by two or more individuals for their respective personal data in the same set of record)
 - **Identity verification**
 - **Specific details** that may help to narrow down the search of the personal data
 - **Access fees** that may be charged to requestors
 - **Response timeframe**
 - **Exceptions** under Fifth Schedule of the PDPA and prohibitions under Section 21 of the PDPA.

The organisation may also consider using an **acknowledgement form** for the requestor to acknowledge the receipt of personal data. Sample access request form and acknowledgement form are provided in the guide.

- When responding to access request from two or more individuals for their respective personal data in the same record, organisations may
 - Provide a **set of all the personal data** to all requestors if consent has been obtained from the respective individuals to disclose their personal data to each other; or

- Provide personal data to each requestor **separately**.
- Organisations should locate the personal data when the access request is received and ensure the personal data is **preserved** while processing the request. For rejected requests, the personal data should be preserved for **minimally 30 days upon rejection**.
In event that PDPC is involved to review the organisation's rejection of access request, the personal data should be preserved till the review is concluded and appeal is exhausted.
- **Record of the access requests received** and the outcomes should be documented. This would help the organisations in the event of a dispute. Such records should only be **retained for the duration** necessary for any legal or business purposes.

Handling CCTV footage access requests

- Organisations may rely on exceptions under Fifth Schedule or prohibitions under Section 21(3) of the PDPA if the access request involves showing CCTV footage of other individuals. However, PDPC is of view that prohibition in Section 21(3)(c)ⁱ of the PDPA would not apply in circumstances where:
 - The other individual has **given consent** to the disclosure of his/her personal data; or
 - Any of the exceptions under the Fourth Schedule of the PDPA apply where organisation may **disclose** the personal data **without consent from the other individual** (e.g. publicly available data); or
 - Organisations are able to provide the CCTV footage **without revealing the personal data of the other individual** (e.g. masking).
- The guidelines are revised such that the organisation may charge an individual a **reasonable** fee (instead of minimal fee) to recover any incremental costs of responding to the access requests.

For more information, please contact:

| | | |
|---|--|---|
| Tan Shong Ye Partner +65 6236 3262 shong.ye.tan@sg.pwc.com | Yap Yee Chin Associate Director +65 6236 3351 yee.chin.yap@sg.pwc.com | Michelle Xie Senior Manager +65 6236 3351 michelle.qy.xie@sg.pwc.com |
|---|--|---|

ⁱ Section 21(3) of the PDPA - An organisation shall not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information, as the case may be, could reasonably be expected to –
(c) reveal personal data about another individual;