CDAC Personal Data Protection Policies and Processes

With effect from 2 July 2014

Contents

1. Background Information

The PDPA was implemented in phases to allow time for organisations to adjust to the new law. The Do Not Call (DNC) Registry provisions came into force on 2 January 2014 and the personal data protection provisions came into force on 2 July 2014.

The data protection provisions govern the collection, use and disclosure of personal data by organisations. In brief, the PDPA contains three main sets of data protection obligations:

- **Obligations relating to notification, consent and purpose**
  Organisations must notify their purposes and obtain consent from individuals for the collection, use and disclosure of individuals' personal data.
- **Obligations relating to compliance, accountability and access and correction**
  Organisations must make information available about their data protection policies, appoint a data protection officer, give individuals access to their personal data (upon request) and allow individuals to correct their personal data (also upon request).
- **Obligations relating to safeguarding personal data**
  Organisation must: (i) comply with prescribed requirements when transferring personal data outside Singapore; (ii) use reasonable measures to protect personal data; (iii) make reasonable effort to ensure the accuracy of personal data; and (iv) cease to retain personal data when no longer required.

The PDPA also provides for the establishment of a DNC Registry. The DNC Registry allows individuals to register their Singapore telephone numbers to opt out of receiving marketing phone calls, mobile text messages such as SMS or MMS, and faxes from organisations.

2. Definition of Personal Data

Personal data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access. Personal data in Singapore is protected under the Personal Data Protection Act 2012.

3. CDAC Personal Data Protection Policy

A standardized Consent statement has also been formulated for all its application forms to ensure that consent is clearly given to CDAC in

handling its personal data and the purpose for which it is utilized. A checklist is also developed to align its practices to the policy.

4. Data Protection Officer

4.1 Appointment of a Data Protection Officer

- The Administration / IT Manager is appointed as the Data Protection Officer, with support by Human Resource Manager to develop CDAC's Personal Data Policies and oversee the CDAC's compliance with the PDPA.

4.2 Roles of the DPO:

- To develop good policies for handling personal data in electronic and/or manual form, that suit CDAC's needs and comply with the PDPA;
- To communicate the internal personal data protection policies and processes to customers, members and employees;
- To handle queries or complaints about personal data from customers, members and employees;
- To alert the management on any risks that might arise with personal data; and
- To liaise with the PDPC, if necessary. Contact point is <info@pdpc.gov.sg>
- To update, change or cancel personal data within 30 days of notice
- To conduct annual audit to ensure that there is no lapse in the CDAC Personal Data Protection policy and processes.

5. Measures and Control to Protect Personal Data

5.1 Administrative Measures

- All staff of CDAC are required to sign and be bound by confidentiality obligations in their employment contracts.
- Should there be a breach of confidentiality, staff may be disciplined or dismissed from their service.
- CDAC conducts regular briefing sessions for staff to impart good practices in handling personal data and strengthen awareness of threats to security of personal data.
- Only appropriate amount of personal data is held by staff for specific functions.

5.2 Physical Measures

- All confidential information must be handled with due care and properly stored/locked when not in use
- Staff could access to confidential documents on a need-to-know basis.
- All unwanted confidential files are disposed through shredding only.

5.3 Information Technology measures

- A yearly review is conducted on these user accounts/rights/roles
- All server data are backed up on a daily basis to offsite
- Only IT / Building Manager have access to the Server premise
- IT infrastructure is protected with Network Firewall, Email Security Firewall, Web Access proxy server and Enterprise Anti-Virus shield