With effect from 2 July 2014

Contents

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) ceased 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.

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.

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.

Data Protection Officer

Appointment of a Data Protection Officer

- The Assistant Director of Data and Research is appointed as the Data Protection Officer, with support by IT Manager, to develop CDAC's Personal Data Policies and oversee the CDAC's compliance with the PDPA.

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.

Measures and Control to Protect Personal Data

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.
- Where data are to be disclosed to partners and contractors for the purpose of managing CDAC's activity, Non-disclosure agreements with the partners/contractors are required to safeguard any data leaks.

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.

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.
- All backup data are encrypted.
- 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.

Handling NRIC Policy

From September 1st, 2019, PDPA Act stipulates that "Organisations are generally not allowed to collect, use or disclose NRIC numbers (or copies of NRIC). They may do so only in the following specified circumstances:

a) Collection, use or disclosure of NRIC numbers (or copies of NRIC) is required under the law (or an exception under the PDPA applies); or
b) Collection, use or disclosure of NRIC numbers (or copies of NRIC) is necessary to accurately establish or verify the identities of the individuals to a high degree of fidelity.

CDAC has identified programmes and schemes that require collection of Full NRIC.

- CDAC - SFCCA Bursary
- CDAC - SFCCA Hardship Assistance Fund
- CDAC Family & Worker Support Programme (All programmes under FSD)
- kidsREAD Programme
- NEU PC Plus Programme
- Home Access Programme
- Programme Fee Subsidy
- Youth Empowerment & Aspiration Programme (YEAP) Grant

There are instances where CDAC will not collect NRIC

- Using of services such as printing and photocopying, internet surfing, library services
- Donors who do not require Tax Exempt receipts
- Opt-Out of CPF Contribution

Retention Policy

CDAC will cease to store or retain any personal data 5 years after the beneficiary ceases to use CDAC services. This is also in line with the 5-year retention period of financial records.

Disposal of electronic and non–electronic data will be done with utmost care bearing the knowledge that an improper disposal can result in a data breach. The software vendor of myCDAC (Crimsonworks Pte Ltd) will be tasked to extract the list of records which have no touchpoints with CDAC for the previous consecutive 5 years for checking before removing the digital data from myCDAC and to provide acknowledgement of the data removal.

Physical documents are disposed by way of shredding. CDAC conducts a shredding exercise every year where we engage a paper recycling company to shred our unwanted documents. CDAC staff will be tasked to follow through the shredding exercise and ensure that a guarantee of destruction certificate is obtained at the end of the exercise.

Handling Data Breach

There are various possibilities of data breaches occurring. Four areas of concerns are internal staff, external hackers, poor disposal practices and internal system malfunction.

a) Internal staff can cause a data breach resulting in data falling into the hands of unauthorized staff. It is also possible for staff with authorized access misusing the data.

b) External hackers pose another challenge as they have vested interest in the data that they want to steal. Such theft can take place if the protection measures are weak.

c) Data disposal if not handled carefully can result in data breaches. Hardcopy data or digital data if not properly disposed of can land on the hands of unintended people.

d) System errors and human errors can also result in data breach. One such example is the recent case of a staff from another organisation sending a list of confidential data to the wrong recipients. This was widely reported in the media and the organization incurred hefty fines as a result. Web sites can have gaps which sometimes can wrongly expose sensitive data to the public. Sufficient security measures must be in-place to prevent this.

Data Breach Management Plan

As a result of the possibilities of breach of information / data, CDAC has developed a set of activities should such an occurrence take place.

CDAC adopts the **CARE** approach to handle data breaches. **C**ontaining the breach, **A**ssessing the risks and impact, **R**eporting the incident and **E**valuating the response and recovery for future breaches.

Containing the Breach

1. Identify the source of the breach
2. Close off the system that was subjected to that breach
3. Prevent any further access by removing access or replacing the rights of the access
4. Establish if recovery of data is required

1. Assessing the Risks & ImpactCDAC will determine the type of data being breached. The level of risks is different for different stakeholders eg Beneficiaries, staff or organization.
2. Determine the risks to reputation, financial, safety or identity to the affected parties
3. Ascertaining the nature of the lost data to determine the notification process to the affected individual
4. By understanding the risks and impact, additional measures can be put in place to mitigate them.

Reporting the Incident

1. Upon detection of a breach, higher management will be immediately notified.
2. The most effective method will be adopted to notify individuals whose personal data have been compromised immediately. This includes guardians or parents of young children whose personal data that have been compromised. Quick notifications may avoid potential abuse of the data.
3. Notify other third parties such as banks, credit card companies or the police, where relevant.
4. Notification will also include how and when the breach occurred and what measures will be taken.
5. PDPC shall be notified especially if a data breach involves sensitive personal data.
6. An Incident report will be raised and the incident documented. Information pertaining to resolution and any other information that is useful for future reference will be documented.

7. Once the breach is resolved, affected individuals will be notified.

Evaluating the Response and Recovery

1. Audits to the system and security measures of CDAC will be carried out regularly to ensure that Data Breach possibilities are minimized or eliminated and that measures are in place to restore or recover should there be a breach.

System Security Review

1. Vulnerability assessment of the organization will be conducted annually
2. Reviews of IT security on regular basis, which will include checks on Firewalls, and Anti-Virus on machines are having the latest updates,
3. Data recovery tests are conducted to ensure information can be restored on demand
4. Clear Data Recovery manual instructions indicating responsibilities and vendors in charge during recovery phase
5. Passwords to our system may be required to be reset upon a Data Breach incident

Post Incident Review

1. CDAC will conduct reviews of any breach to staff so that there is awareness of the breach and if so, the learning points takeaway from the incident
2. If the breach was due to poor judgement, errors or wrong job execution of staff, decision has to be made for additional staff training on personal data protection awareness.
3. Where a breach has occurred, higher management must be made aware and that clear line of responsibility and communication must be established

Handling Complaints

If there is a mishandling of personal data, and is felt that the organization has breached the Personal Data Protection Act, the affected individual can fill the Complaint Form and submit it to the Data Protection Officer.

CDAC will review the information provided on the submitted complaint form and to work with higher management as well as the relevant department in charge of the programme to review the facts and determine if indeed there is merit in the complaint.

CDAC will decide the course of action to take and to inform the complainant on the outcome of the investigation as well as the course of action to be taken.

PDPA Complaint Form

If you have complaints concerning CDAC's handling of your data, fill up the form and submit it to the Data Protection Officer (dataprotection@cdac.org.sg)

Your contact details

Name	
Contact Number	
Email Address	

Which CDAC's programme /business unit are you involved with

Corporate Service	
Fulfilling Ageing	
Family & Worker Support	
Community Outreach & Engagement	
Student & Parent Education	
OneStop Service	
Others	

Description of complaint

Please note that during the investigations, CDAC may need to contact you for additional information or share the information provided to help complete the investigation process.

The information provided by you is necessary for processing your complaint and any inaccuracies, errors or omissions in the personal data submitted may result in delays or inability to process your request.

PDPA INCIDENT REPORT

Recorded by	
Date of Incident	
Incident Description	
Severity	
Source of Incident	
Duration of Outage	
Remedial Action	
Control Measure	