Block 50 Commonwealth Drive #01-506 Singapore 142050

Data Protection Policy

CONTENTS **PAGE**

A. Introduction

Personal Data Protection Act (PDPA) was passed by the Parliament in October 2012. It is a new data protection law comprises various rules governing the collection, use, disclosure and care of personal data. It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes. The law safeguard consumers' personal data against misuse.

The Act includes the Do Not Call (DNC) Registry, in which the individuals are given the choice to opt out of receiving marketing phone calls, mobile text messages such as SMS and faxes from organisations.

B. Objective

To ensure that FaithActs complies with the Personal Data Protection Act 2012 (PDPA) in the collection, use, disclosure, maintenance of accuracy, handling and security of personal data in a manner that recognises both the right of individuals to protect their personal data and the need of the organisation to collect, use and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

C. Scope

The policy defines the responsibilities of FaithActs in ensuring compliance to the PDPA by executing good control and consistency in the collection, usage and disclosure of personal data.

D. Appointment

FaithActs will appoint a Data Protection compliance officer.

E. General principles

1. Responsibility: FaithActs shall be responsible for personal data in its possession or under its control. "Personal data" means 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.

2. Consent: Get consent to collect, use or disclose personal data. Written or actual consent should be sought but if not ensure at least ensure that there is deemed consent. See part C.

3. Use: Only use or disclose personal data use or disclose personal data about an individual for the purposes for which the data was obtained. Always ensure that use is objectively reasonable and extent of use limited to carrying out purpose.

4. Access to personal data: Seek to ensure that the individual has reasonable (and justified access to his or her personal data) and has an opportunity to correct it. See part E.

5. Care of personal data: Seek to ensure that personal data accurate, properly protected, properly retained (and accessible by authorised or appropriate person/s).

F. Consent

1. Note the general principles.

2. When collecting information (e.g. in registration forms) clearly state and seek consent for the following:

   - the purpose for the collection of data collected.
   - the usage of the data collected.
   - the ways the personal data will be disclosed.
   - the contact information of a person who is able to answer on behalf of FaithActs the individual's questions about the collection, use or disclosure of the personal data.

3. For deemed consent, ask following questions (only yes answers acceptable):
   (a) Has the individual voluntarily provided the personal data for the purpose for which it is to be used?
   (b) It is reasonable that the individual would voluntarily provide the data?

4. Seek consent where personal data is to be passed on to another organisation. Written consent preferred, but if not, ensures that there is deemed consent.

5. Do note that consent can be withdrawn. When withdrawn, FaithActs should inform the individual concerned of the likely consequences of withdrawing his consent.

G. Access

1. Follow principles.

2. Ensure access by individual. Verify who the individual is.

3. As a rule reasonable access must be given but not if the provision of that personal data or other information, as the case may be, could reasonably be expected to —

   (a) threaten the safety or physical or mental health of an individual other than the individual who made the request;

   (b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;

   (c) reveal personal data about another individual;

   (d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the

disclosure of his identity; or

(e) be contrary to the national interest.

4. Allow reasonable opportunity to rectify incorrect information. When corrected, FaithActs send corrected info to any other organisation provided incorrect information within a year of correction, unless that other organisation does not need the corrected personal data for any legal or business purpose.

H. Care:

- **Confidentiality**

  – FaithActs will keep all personal data confidential and accessible to only authorised and need-to-know personnel.

- **Staff Working Area**

  Staff working area must be secure. This includes:
  – Work desks
  – Meeting/ Discussion areas
  – Filing cupboards
  – Printers
  – Fax machine
  – Pass word protected

  Access to work areas must be through locked doors such that other staff and visitors do not have access to such areas.

- **Databases and registration files/forms**
  – Soft copy databases must be password protected where applicable and stored in the dedicated ministries.
  – Access to the softcopy databases should only be given to authorized staff of WMC.
  – All staff is not allowed to save any copies of databases in their own computer hard drives or portable storage drives.
  – Records of members/friends for the collection, usage and disclosure (or withdrawal of) must be informed and kept with the membership and database officer.
  – Hardcopy registration files/forms containing personal information must be kept strictly under the ministries' care in locked cupboards.

  Due care should be taken to ensure that personal data is protected, secured and accessible by the appropriate person(s). To this end, appropriate measures should be taken.

I. Do note the exceptions, one of which is where the collection and use of data is necessary to response to an emergency that threatens the life/health or safety of the individual or another individual. For more exceptions, discuss with the administrator.

Donors	Administrator
Volunteers	Volunteer Management Staff and Youth Worker
Clients	Social Workers/Case Workers
	Standard Operating Procedures (some examples)
Donors	1. Personal data are collected for the purpose of issuing official receipts for donation received from fund raising which are clearly stated in all the collaterals. 2. Donors and Sponsors are given an option to remain anonymous or consent to having their names printed in all collaterals. 3. In the event the donor's/sponsor's particulars are disclosed verbally, the time and date of the conversation is recorded for future reference with an email confirmation wherever possible. 4. All personal data is saved in our digital file. This database is password protected and is known only to the staff administering the database and the fundraising manager. The hard copies are filed and kept accessible only to the staff administering the database and the fundraising manager. 5. In the event that the donor/sponsor requests to be removed from our record, the name and all data pertaining to the donor/sponsor will be removed from the database. 6. In the case of a donor/sponsor passed on, all data will be removed from the database and recorded in the archive database. All hard copies will be archived. 7. Personal data or details are private and confidential and will not be released other than that which is in accordance to our purpose. 8. In the event that the computer holding the database is replaced the hard disk of the computer will be formatted and cleaned. 9. Use and disclosure of personal data is only for the purpose that the data is obtained. 10. FaithActs do not collect data from any data intermediary or third parties.
Volunteers	Personal data are collected for the purpose of sending birthday and festive greetings and duty roster. Observe principles!
Clients	Steps are taken to ensure clients' files are properly handled. In the event the file is lost or misplaced, the Data Protection Compliance Administrator will be informed and a police report made. Case files are kept in locked cabinet and only the case workers in charge of the respective case will have access to the case files. Observe principles at all times. Special care needs to be taken for clients.

Appendix

Privacy Policy and Consent to Use of Data

By interacting with, submitting information to or signing up for any organised activity offered by FaithActs, you agree and consent to FaithActs collecting, using, disclosing and sharing amongst the relevant departments your personal data, for the purpose of engagement, operational planning of activities, as well as communication of events, programmes and centre-related information. FaithActs respects personal data and privacy, and will not share such information with any third party. Should you wish to withdraw or limit your consent, please write with full particulars to our Data Protection Compliance Officer:

FaithActs
Block 50 Commonwealth Drive #01-506
Singapore 142050
Tel: 6339 7611
Email : info@faithacts.org.sg