TomoWork Ltd

Data Protection Policy

TABLE OF CONTENTS

Manual Implementation and Review

Effective date	7 Dec 2022
Approved by	Board of Directors
Document owner	Data Protection Officer

Version history					
Date	**Version**	**Updates** *(List details of updates i.e. Section and Details)*	**Updated by** **(Name / Title)**	**Reviewed by / Date**	**Approved by / Date**
11 April 2022	**Version 1.0**	**New**	**Shared Services for Charities Ltd**	**Data Protection Officer / 8 April 2022**	**Board of Directors / 8 April 2022**
7 Dec 2022	Version 2.0	Business Contact Information of DPO	Masako Yanagiya DHFG	Data Protection Officer / 7 Dec 2022	Board of Directors / 7 Dec 2022

1 INTRODUCTION

1.1 Definition

1.1.1 Personal Data refer to data, whether true or not, about an individual who can be identified:

a) From the data; or

b) From that data and other information to which the organisation has or likely to have access.

1.1.2 This is a very broad definition which covers almost any kind of data. It can include photographs, videos, voice recordings, names, addresses, education and employment details, and even stories about what has happened to a person. Hence, you should take care when dealing with any form of information about any individual as it could potentially fall under the definition of personal data – and therefore be protected by and subject to the Personal Data Protection Act.

1.2 Definition of Terms

1.2.1 The following abbreviations herein bear references to the following:

Term	Abbreviation
TomoWork Ltd	TOMO
Board of Directors	the Board
Chief Executive Officer	CEO
Director of Finance, HR and Governance	DHFG
Personal Data Protection Act	PDPA
PDPA Manual	the Manual
Data Protection Officer	DPO
Data Protection Impact Assessment	DPIA
Curriculum Vitae	CV

1.2.2 Whenever used herein, the singular number shall include the plural, the plural shall include the singular, and the use of any gender shall include all genders.

1.3 Exclusions

1.3.1 The following scope are excluded from the Manual:

a) Do Not Call Registry; and

b) Business contact information, meaning an individual's name, designation or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for their personal purposes.

1.4 Objectives and Scope

1.4.1 This Manual:

a) Sets up the policies and procedures to be applied in the collection, recording, use, retention and safeguarding of personal data for TomoWork Ltd ("TOMO");

b) Sets up the roles and responsibilities of the DPO;

c) Provides a clear understanding of the lines of authority and responsibilities over the collection, recording, use, retention and safeguarding of personal data; and

d) Facilitates compliance with the PDPA 2012.

1.5 Purpose and Application

1.5.1 The PDPA applies to all organisations, including Social Service Agency such as TOMO. Organisations are required to comply with the PDPA by establishing practices and policies to meet its data protection standards. Any party committing an offence under the PDPA can face fines of varying amounts, based on the severity of the offence.

1.5.2 The Manual serves as a reference and training document for Management and staff.

1.5.3 Management and staff shall refer to the relevant section of the Manual for guidance in the execution of their daily operations. Compliance to the Manual is compulsory for all Management and staff.

1.6 Approval and Changes

1.6.1 This Manual shall be effective upon approval by the Board.

1.6.2 This Manual shall be reviewed when there is a change in the PDPA and/or policy & procedures.

1.6.3 Changes to the Manual shall be recommended by the DPO and shall take effect upon approval by the Board.

1.6.4 All changes shall be communicated to the Management and staff for the purpose of awareness and adherence at all times.

2 DATA PROTECTION FUNCTION

2.1 Appointment and Delegation

2.1.1 The DPO shall be appointed by the Board. An Appointment Letter, stating the roles and responsibilities of the DPO shall be issued to the DPO before the date of effect.

2.1.2 DPO shall delegate his role and responsibilities before any leave of absence for three (3) days or more consecutive working days to an appointed staff. DPO shall notify all staff of the delegation, including the name of the staff appointed and the period of delegation.

2.2 Business Contact Information of DPO

2.2.1 The business contact information of the DPO is as follow:

a) Email: enquiry@tomowork.org

b) Contact number: 8123 - 2192

c) Mailing Address: Cross Street Exchange, 18 Cross Street, #02-101, Singapore 048423

2.2.2 DPO shall ensure that the business contact information released to the public is updated at all times.

2.2.3 DPO shall ensure that a response is made to the individual, either through email, letter or phone call, within three (3) working days upon receipt of an enquiry / complaint through any of the above modes.

2.3 Roles and Responsibilities

2.3.1 The roles and responsibilities of the DPO shall be as follows:

a) Develop and implement policies and procedures that are necessary for TOMO to meet its obligations under the PDPA 2012;

b) To communicate policies and procedures to Management and staff;

c) To be the contact point between TOMO and individuals, and to answer on behalf of TOMO on queries relating to personal data;

d) Make available policies and procedures on collection, use, disclosure and storage of personal data or complaints process to individuals, on request;

e) Ensure training is conducted for all staff, including volunteer, upon commencement and at least one (1) refresher training to be conducted for existing staff annually;

f) Ensure TOMO protects personal data by making reasonable security arrangements to prevent unauthorised actions; and

g) Ensure that personal data are not retained longer than necessary.

2.3.2 The DPO shall also refer to the general guides released by Personal Data Protection Commission ('PDPC') from time to time, in addition to the following:

a) Advisory Guidelines for the Social Service Sector (Revised on 31 August 2018); and

b) Advisory Guidelines on Key Concepts in the PDPA (Published on 1 Oct 2021).

3 TRAINING AND COMMUNICATION

3.1 Training Plan

3.1.1 TOMO is committed to be provide training on PDPA for its staff and has established the following training plan for its staff.

3.1.2 Trainings are categorised based on their job requirements.

*Refer to **Appendix 1** for the Training and Communications Plan*

3.1.3 All staff are required to complete the PDPC e-learning assessment on a yearly basis. The DPO is to send out the assessment link and track the completion of assessment by all staff.

4 DATA PROTECTION IMPACT ASSESSMENT

4.1 General Principles

4.1.1 TOMO is committed to be proactive and takes systematic approach in adopting appropriate measures and tools to address specific personal data protection risks and its needs by conducting DPIA.

4.1.2 A DPIA involves identifying, assessing and addressing personal data protection risks based on TOMO functions, needs and processes.

4.2 When to conduct a DPIA

4.2.1 TOMO conducts DPIA for the following:

a) Website;

b) Systems (e.g. Servers, software);

c) Cloud storage platforms;

d) Key processes involving personal data.

4.2.2 DPIA is conducted under the following circumstances:

a) Implementation of new system;

b) Implementation of new process involving personal data;

c) Change in process within an existing system;

d) Change in organisational structure that handles personal data.

4.3 Conducting a DPIA

4.3.1 The DPIA must be conducted by the following staff:

a) Project Lead;

b) DPO;

c) DPIA Approving Authority;

d) Any other affected staff.

4.3.2 The DPIA team shall perform the following:

a) Identify personal data handled by the system or process, as well as the reasons for collecting the personal data

b) Identify how the personal data flows through the system or process

c) Identify data protection risks by analysing the personal data handled and its data flows against PDPA requirements or data protection best practices

d) Address the identified risks by amending the system or process design, or introducing new policies

e) Check to ensure that identified risks are adequately addressed before the system or process is in effect or implemented

4.3.3 The DPIA performed shall be documented in DPIA report. The DPIA Report shall be approved by the Board.

*Refer to **Appendix 2** for the DPIA Report Template*

4.3.4 At the end of each DPIA, the DPO shall record the DPIA performed in the DPIA Log.

*Refer to **Appendix 3** for the DPIA Log*

4.3.5 The following PDPC general guides shall be referred to for more information on conducting a DPIA:

a) Guide to Data Protection Impact Assessments (Revised on 14 September 2021).

5 COLLECTION, USE, DISCLOSURE AND STORAGE OF PERSONAL DATA

5.1 General Principles

5.1.1 TOMO shall collect, use, disclose or store personal data from or about an individual for purposes that a reasonable person would consider appropriate in the circumstances.

5.1.2 TOMO shall notify the individual of the purpose for collecting, using or disclosing the personal data before obtaining expressed consent from the individual.

5.1.3 TOMO collects personal data from various channels. These include, but not limited to/from:

a) Conference recordings within and outside TOMO premises;

b) Photos and video recordings at TOMO events (within and outside TOMO premises);

c) Beneficiaries ("Members") and their families;

d) Job, Internship, and Volunteer opportunity;

e) Cash and/or In-kind donations to TOMO;

f) Interaction/Meeting with TOMO's staff, community partners, interns, volunteers, board and committee members.

g) Interaction/engagement, i.e., outreach, done face to face or by other means with community members (individuals within and outside of TOMO service boundary).

5.1.4 Should there be a change in or addition of the purpose for the collection of personal data, TOMO shall inform the individual and seek consent for the other purpose(s), before using or disclosing the personal data.

5.1.5 Personal data which was collected before consent was sought shall be used only for the purpose(s) for which it was collected.

5.1.6 TOMO shall rely on an individual being deemed to have consented to TOMO collecting, using, disclosing and storing personal data about the individual:

a) When the individual makes a donation to TOMO;

b) When the individual receives services from TOMO;

c) When the individual interacted/engaged with TOMO, e.g., outreach;

d) Photographs and video recordings under certain circumstances;

e) Video recordings from CCTV cameras operated by or for TOMO; and

f) When seeking employment or volunteering with TOMO; and

g) The individual's transaction includes contractual necessity.

5.1.7 TOMO shall accept consent from another person[N1] on behalf of an individual under the following circumstances:

a) Individual is a minor i.e. individual who is less than 21 years of age; or

b) Individual lacks the intellectual capacity to provide such consent.

**N1: A parent or a legal guardian of the individual is ordinarily such a person. The DPO may request for a copy of the Court Order from the legal guardian.*

5.1.8 The individual may withdraw their consent for TOMO to collect, use and disclose the personal data at any point of time, even if prior consent had been obtained.

5.1.9 TOMO does not transfer any personal data to any countries or territories outside Singapore. Should TOMO transfer any personal data to a country or territory outside Singapore, TOMO shall ensure that the standard of protection accorded to the data transferred is comparable to the protection under PDPA.

5.1.10 The following PDPC general guides shall be referred to for more information on the collection, use, disclosure and storage of personal data:

a) Guide to Notification (Published on 26 September 2019);

b) Guide to Preventing Accidental Disclosure When Processing and Sending Personal Data (Published on 20 January 2017); and

c) Guide to Data Sharing (Revised on 1 February 2018).

5.2 Members' and Community Members' Personal Data

5.2.1 Members refer to beneficiaries or clients receiving assistance or support from TOMO. Community members refer to individuals from the community that TOMO engages.

5.2.2 TOMO shall collect personal data of an individual through the following ways:

a) Referrals (e.g. government agencies, public);

b) Applications of TOMO programmes and services; or

c) Community outreach.

5.2.3 TOMO shall ensure consent is obtained from the individual for personal data that were received through consent forms and/or from third party.

5.2.4 TOMO does not disclose the personal data received or collected for any other purposes, other than for the purpose of providing services for the individual.

5.3 Board and Sub-Committee Members' Personal Data

5.3.1 TOMO collects personal data of its Board and Sub-Committee Members, who are also volunteers.

5.3.2 TOMO shall obtain deemed consent from individual new Board or Sub-Committee Member for the specified purposes for the collection, use and disclosure of the personal data.

5.3.3 TOMO shall use and disclose the personal data collected for the following purpose(s):

a) Appointment to the Board and/or Sub-Committee;

b) Re-appointment to the Board and/or Sub-Committee; or

c) Removal from the Board and/or Sub-Committee.

5.4 Donors' Personal Data

5.4.1 TOMO collects personal data of donors through the following ways:

a) Online donation platforms;

b) Mail-in donations; or

c) Walk-in donations.

5.4.2 TOMO relies on the donor being deemed to have consented to TOMO collecting, using and disclosing the personal data:

a) When a donation is made;

i) Submission of their name and NRIC to Inland Revenue Authority of Singapore for tax deduction purposes; and

ii) Contact information for clarification or resolution of query with regards to the donation made.

b) Name, email address or mailing address for the purpose of sending the tax deduction receipt.

5.4.3 TOMO shall obtain separate consent from the individual for the purpose of future communications (e.g. newsletters, events).

5.5 Staff's Personal Data

5.5.1 TOMO collects personal data of staff through various stages of employment. TOMO shall not collect, use or disclose personal data of an individual without prior consent.

5.5.2 Recruitment

a) Personal data is collected through the Employment Application Form, which shall be completed and signed off by the applicant. This provides expressed consent to TOMO for the collection, use and disclosure of personal data from the applicant.

b) The applicant is deemed to have consented if:

i) Their CV is sent to TOMO directly; or

ii) Their CV is made available on a job search portal.

c) TOMO requires applicant to nominate referees and to provide the referees' personal data, i.e. contact number. TOMO shall deem that consent had been obtained by the applicant from the referee for the disclosure.

d) Consent from the applicant is not required if:

i) The personal data is publicly available information. For example, social networking platforms; or

ii) The personal data is for evaluative purposes. For example, TOMO may obtain reference from the applicant's former employer or business colleagues to evaluate their suitability for employment.

5.5.3 Appointment

a) The successful applicant shall provide further details (e.g. NRIC and bank account details) prior to or upon commencement of work.

b) Personal data which was provided by the individual shall be used for the sole purpose of managing the employment relationship with the individual.

5.5.4 Consent from the staff for collection, use and disclosure is not required if:

a) The personal data is publicly available information;

b) If there is an emergency; or

c) The disclosure is related to law enforcement.

5.5.5 TOMO shall inform the staff on the purposes for collecting their personal data, which may include but not limited to:

a) Use of bank account details for payroll;

b) Managing staff benefit schemes, i.e. training, insurance, medical; or

c) Managing / termination of employment.

5.6 Volunteer's Personal Data

5.6.1 TOMO shall collect personal data of a volunteer through the following ways:

a) Volunteer Application Form; or

b) Application for volunteering by a partner organisation.

5.6.2 TOMO shall deem that consent had been obtained by the organisation from the volunteer for personal data that were received through the partner organisation.

5.6.3 TOMO does not disclose the personal data received or collected for any other purposes, other than for the purpose of volunteering in TOMO.

5.6.4 TOMO shall obtain separate consent from the individual for the purpose of future communications (e.g. newsletters, events).

5.7 Data Intermediaries

5.7.1 Data intermediary refers to an organisation which processes personal data on behalf of TOMO but does not include a staff.

5.7.2 Personal data provided by TOMO to the data intermediary remains under the control of TOMO.

5.7.3 When engaging a data intermediary, TOMO should:

a) Achieve a reasonable level of assurance that the data intermediary has policies, procedures and controls in place to ensure compliance with PDPA; and

b) A contract in writing shall be signed between TOMO and the data intermediary that clearly specifies the data intermediary's obligations and responsibilities in order to ensure TOMO compliance with PDPA.

5.7.4 The following PDPC general guide shall be referred to for more information on data intermediaries:

a) Guide on Data Protection Clauses for Agreements Relating to the Processing of Personal Data (Published on 1 February 2021).

5.8 Photographs and Video Recordings

5.8.1 The image of an individual in a photograph or video recording, including a CCTV recording or any other method of capturing images, held by TOMO shall be personal data of that individual if the individual is identifiable from that image by TOMO.

5.8.2 Personal data shall be considered publicly available if it can be observed by reasonably expected means at a location or event which the individual appears and that is open to the public.

5.8.3 Personal data shall only be collected through photography or videography only if:

a) DPO had confirmed that the relevant personal data shall be publicly available information;

b) Each identifiable individual shall deem to have consented to the collection of personal data;

c) Each identifiable individual has provided expressed consent to the collection of personal data; or

d) The staff has sought and received consent in writing from the DPO, on a case by case basis.

5.8.4 TOMO should take reasonable steps to avoid collecting personal data of an individual by photography or videography where the individual has withdrawn their consent.

5.8.5 TOMO shall notify the individual of the purpose for which the photograph or video is taken. The purpose may be notified through the following ways:

a) Invitations to the event organised, which a clear statement that photographs or videos will be taken for the specific purposes;

b) An obvious notice to be placed at the reception / registration table / entrance of the venue to inform attendees that photographs or videos will be taken for the specified purposes; or

c) The photographer / videographer to inform the individuals the purpose of taking the photograph / video recording if the individual is asked to pose for the photographs / videos.

5.8.6 TOMO shall rely on an individual being deemed to have consented to the collection, use and disclosure of personal data under the following circumstances:

a) The individual poses for a photograph or video recording at the request of the photographer / videographer;

b) TOMO has notified the individual the purposes for which it collects, use or disclose the personal data;

c) Indicate clearly in the invitation or registration documents send or made available to participants; or

d) The individual has accepted invitation or registered to indicate their participation in the event.

5.9 Disclosure

5.9.1 TOMO may collect, use and disclose personal data about an individual without their consent under the following emergency circumstances:

a) In emergency situations that threatens the life, health or safety of the individual or another individual;

b) Purpose of contacting next-of-kin or a friend of any injured, ill or deceased individual; or

c) Reasonable grounds to believe that the health or safety of the individual or another individual will be seriously affected and consent for the disclosure could not be obtained in a timely manner. The staff shall notify the DPO in writing:

i) The circumstances surrounding the emergency situation;

ii) The manner which the staff used the relevant personal data; and / or

iii) The identity of the individual and / or organisation which the staff disclosed the personal data to.

5.9.2 TOMO may also disclose personal data to any officer of a prescribed law enforcement agency upon production of written authorisation, without the individual's consent:

a) Signed by the head of the law enforcement agency; and

b) Certifying that the personal data is necessary for the purposes of the functions of duties of the officer.

c) The staff shall notify the DPO immediately should such authorisation is received.

5.9.3 The DPO may also seek legal advice to determine the extent to which TOMO is required to provide the personal data requested by the law enforcement agency.

5.9.4 Any collection, use or disclosure of personal data by TOMO for legal purposes shall only be done if:

a) By / under supervision of the DPO;

b) At the DPO's / legal counsel's request; or

c) As directed by the CEO, or in his absence, Chairman of TOMO.

All staff must refer any legal matter to DPO, or in their absence, the CEO, immediately.

5.9.5 Any collection, use or disclosure of personal data by TOMO to the public agency shall only be done if:

a) The DPO is satisfied that the organisation requesting the personal data is a public agency, within the meaning of the PDPA; and

b) The disclosure is necessary in the public interest.

The DPO shall obtain legal advice before providing such approval, except where the Chairman of TOMO determines it is not necessary.

5.9.6 Records shall be maintained by the DPO on all requests made, with the following details:

a) The date which TOMO received the request;

b) The party making the request;

c) The type of personal data released; and

d) Any relevant legal advice provided, if any.

6 WITHDRAWAL OF CONSENT

6.1 General Principles

6.1.1 Upon giving reasonable notice, an individual may at any time withdraw any consent or deemed consent given, in the collection, use or disclosure of personal data for any purposes.

6.1.2 All notifications of withdrawal of consent shall be referred to the DPO. The DPO may require the DP Committee to handle the request.

6.1.3 The DPO/ staff in charge is to respond to the individual's request within ten (10) working days. Where not possible, TOMO shall inform the individual of the timeframe.

6.2 Proof of Identity

6.2.1 DPO shall undertake reasonable steps to ensure that the proof of identity is provided by the individual for the withdrawal of consent. DPO has the discretion to waive or vary an identification requirement on a case by case basis.

Category of individual	Proof of identity
Members	Name, NRIC and contact number
Community Members	Name and contact number
Donors	Name, NRIC and contact number
Ex-Staff	Name, NRIC and contact number
Volunteers	Name and contact number
Board and Sub-Committee members	Name and contact number

6.2.2 Under the circumstances whereby a person acts on behalf of an individual, under legal authority, the person shall produce proof of their identity, and at the discretion of the DPO, their authority to act on behalf of the individual.

6.2.3 If the DPO is not satisfied with the proof of identify but has no reason to suspect the individual and the withdrawal of consent would or not likely to have adverse consequences, the DPO shall proceed to notify the individual on the consequences of withdrawal of consent.

6.2.4 If the DPO is not satisfied with the proof of identity and the withdrawal of consent would or likely to have adverse consequences, the DPO shall perform the following steps:

a) Try to contact the individual concerned;

b) Explain to the individual that TOMO needs to guard the possibility of consent being withdrawn improperly and without knowledge of the individual; and

c) Request for further or additional proof of identity.

If the individual is uncontactable or is not willing to provide further or additional proof of identity, DPO shall have the discretion not to withdraw the consent provided on the collection, use or disclosure of the personal data.

6.3 Notification of Consequence

6.3.1 Upon satisfactory confirmation of the identity of the requester, DPO or his delegates shall inform the individual within three (3) working days on the consequences of withdrawing consent, either through email or letter.

6.3.2 DPO or his delegate may provide information of the consequences of withdrawal verbally. However, a written confirmation shall still be provided to the individual.

6.4 Follow-up Actions

6.4.1 The DPO shall notify the staff in charge to ensure that TOMO and any data intermediary ceases to collect, use or disclose the personal data for the purpose in which the individual had withdrawn.

6.5 Records

6.5.1 The DPO shall maintain records of the withdrawal of consent of the individual, with the following details:

a) The date which TOMO received the notice or indication of withdrawal of consent;

b) The name of the individual making the request;

c) The mode in which the notification is made, i.e. email, phone call;

d) Type of proof of the identity of the individual making the request;

e) Date and contents of information provided about the consequences of withdrawing consent; and

f) A copy of notification to staff and any data intermediary to cease the collection, use and disclosure of the relevant personal data.

7 ACCESS TO PERSONAL DATA

7.1 General Principles

7.1.1 An individual may request for access about the use of their personal data in the organisation, through notification to the DPO.

7.1.2 All requests shall be referred to the DPO immediately. For staff's request to access their personal data, the request shall be directed to the DFHG.

7.1.3 The DPO shall provide the requested access to the extent necessary to the individual. The DPO may also authorise a staff to handle the request.

7.1.4 The DPO shall respond to the individual within thirty (30) days, upon receipt of the request, on the status of the request. Where not possible, TOMO shall inform the individual of the timeframe.

7.1.5 The following PDPC general guides shall be referred to for more information on the access requests to personal data of an individual:

a) Guide to Handling Access Requests (Published on 9 June 2016); and

b) Guide to Basic Data Anonymisation Technique (Published on 25 January 2018).

7.2 Proof of Identity

7.2.1 The DPO shall send the Access Request Form to the individual for completion.

*Refer to **Appendix 4** for the Access Request Form*

7.2.2 Please refer to section 6.2 on the policies and procedures pertaining to the proof of identity.

7.2.3 If the DPO is not satisfied with the proof of identity provided, the DPO shall have the discretion not to accede to the request for access.

7.3 Follow-up Actions

7.3.1 Upon satisfactory confirmation of the identity of the requester, the DPO shall proceed to determine if exemptions or prohibitions applies.

7.3.2 If the DPO is satisfied that no exemption or prohibition applies to the request, the DPO shall:

a) Provide a copy of the personal data requested to the email address or mailing address specified by the individual. The DPO shall ensure that there is no personal data of another individual in the document provided.

b) Provide the information on the use or disclosure made about the personal data to the email address or mailing address specified by the individual.

7.3.3 Upon providing the personal data or information requested, the DPO shall obtain acknowledgement from the requestor for the personal data or information received.

*Refer to **Appendix 5** for the Acknowledgement of Personal Data Received for an Access Request Form*

7.3.4 If the DPO determines that exemption applies, the DPO has the discretion to provide the requested access of personal data or information, taking into consideration the circumstances as described in section 7.4.

7.3.5 If the DPO determines that prohibition applies, the DPO shall not provide access to the personal data or information to which the prohibition applies, taking into consideration the circumstances as described in section 7.5.

7.3.6 If the DPO determines that exemption or prohibition only applies to part of the personal data which the individual had requested, the DPO shall provide partial access to the personal data or information.

7.4 Circumstances for Exemptions

7.4.1 It is not compulsory for the DPO to provide an individual with access to personal data or information for the following circumstances:

a) Opinion data that is kept solely for evaluation purpose;

b) Legal matters in respect to:

i) A document related to a prosecution if all proceedings related have not been completed; or

ii) Personal data collected, used or disclosed without consent for the purposes of an investigation, which the investigation and associated proceedings and appeals have not been completed.

c) Unreasonable requests such as:

i) The request would unreasonably interfere with the operations of TOMO due to the repetitious or systematic nature of the requests;

ii) The burden or expenses of providing access would be unreasonable to TOMO or disproportionate to the individual's interest;

iii) Information that does not exist or could not be found;

iv) Information that is trivial; or

v) Information that is otherwise thoughtless or troublesome.

7.4.2 For access request where legal matters are involved, the DPO shall seek specific legal advice to:

a) Confirm whether the specific personal data and information falls within the exemption;

b) Understand the possible implications of TOMO voluntarily providing access to the requested personal data or information on its use or disclosure; and

c) Inform the individual for the reason for the decline of request, taking into consideration on the legal implications connected with the legal matter.

7.5 Circumstances for Prohibitions

7.5.1 TOMO shall not provide the personal data or information about its use or disclosure under the following circumstances if DPO could reasonably expect that the information:

a) Threatens 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 physical or mental health of the individual who made the request;

c) Reveal personal data of another individual; or

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 their identity.

7.5.2 If the request is made by a person who has legal authority to act on behalf of the individual, TOMO shall not provide the individual's personal data or information about its use and disclosure if the DPO could reasonably expect any of the above consequences, as mentioned in section 7.5.1.

7.5.3 If personal data is disclosed to a law enforcement agency or law enforcement officer, TOMO shall not inform the individual that:

a) Their personal data had been disclosed to a law enforcement agency for any investigations or proceedings; or

b) Their personal data had been disclosed to a law enforcement officer, who had produced a written authorisation certifying that the information was necessary for the purposes of the functions or duties of the officer.

7.6 Records

7.6.1 The DPO shall maintain records of the requests for access to personal data or information about the use and disclosure, with the following details:

a) The date which TOMO received the request;

b) The name of the individual making the request;

c) The mode in which the request is made, i.e. email, phone call;

d) Whether the request is for access to personal data or for information on the use or disclosure of the personal data or both;

e) Type of proof of the identity of the individual making the request;

f) The date which the DPO accede or decline the request;

g) The reasons and reasonable steps taken should the request be declined; and

h) Legal advice obtained, if any.

8 CORRECTION OF PERSONAL DATA

8.1 General Principles

8.1.1 An individual has the right to request TOMO to correct an error or omission in the personal data about the individual that is in possession or under the control of TOMO. However, there are circumstances whereby TOMO need not correct the personal data.

8.1.2 All requests shall be referred to the DPO immediately. For staff's request to correct their personal data, the request shall be directed to the DFHG.

8.1.3 The DPO shall consider if a correction should be made and either make the correction or authorise a staff to make the correction.

8.1.4 The DPO shall respond to the individual within thirty (30) days, upon receipt of the request, on the status of the request. Where not possible, TOMO shall inform the individual of the timeframe.

8.2 Proof of Identity and Evidence of Error or Omission

8.2.1 The DPO shall send the Correction Request Form to the individual for completion.

*Refer to **Appendix 6** for the Correction Request Form*

8.2.2 An individual shall provide proof of identify and evidence of the error or omission which they request to be corrected.

8.2.3 Please refer to section 6.2 for further details on the proof of identity.

8.2.4 If the DPO is not satisfied with the proof of identity, the DPO shall have the discretion not to correct the error or omission of the personal data.

8.3 Follow-up Actions

8.3.1 Upon satisfactory confirmation of the identity of the requester, DPO shall:

a) Extract the personal data from TOMO records;

b) Determine if any exceptions to correct any error or omission apply; and

c) Check if TOMO has disclosed the personal data to any other organisation(s) within a year from the date of requested correction, and if so, the purpose of the disclosure(s).

8.3.2 If no exceptions apply, DPO shall

a) Examine the evidence supporting the request to correct the personal data;

b) Determine whether the requested correction should not be made on reasonable grounds; and

c) Respond to the individual making the request that:

i) TOMO has made the correction and/or if applicable, requested its data intermediary to make the requested correction;

ii) TOMO is not required to make the correction due to an exception, citing the applicable exception; or

iii) TOMO is satisfied that the correction should not be made, citing the reasons for reaching that conclusion, and if appropriate to request the individual to provide TOMO with further information supporting the request for the correction of personal data.

8.3.3 Upon confirmation of the correction request, the DPO shall obtain acknowledgement from the requestor for the personal data or information corrected.

*Refer to **Appendix 7** for the Acknowledgement of Personal Data Correction Form*

8.3.4 If an exception applies, DPO shall notify the individual that TOMO is not required to correct the relevant personal data.

8.3.5 DPO may provide the response in writing or verbally. However, a written response shall still be provided to the individual.

8.3.6 If the corrected personal data had been disclosed to any other organisation(s) within a year of the date of correction, the DPO shall:

a) Decide if the organisation(s) needs the corrected personal data for any legal or business purpose; and

b) Send a written notice of correction, including reasons for the correction and / or evidence to support the correction, to the organisation(s).

8.3.7 If TOMO receives a notification of corrected personal data from another organisation, TOMO shall correct the personal data in the possession or under the control of TOMO, unless the DPO is satisfied on reasonable grounds that the notified correction should not be made. DPO shall maintain the records and note that the required correction was not made.

8.4 Circumstances for Exemptions

8.4.1 DPO shall not be required to make corrections to the following:

a) Opinion data kept by TOMO solely for evaluative purposes;

b) Opinion made by TOMO or professional or expert; and

c) Document relating to a prosecution if all proceedings related have not been completed.

8.5 Records

8.5.1 The DPO shall maintain records of the requests for correction to personal data, with the following details:

a) The date which TOMO received the request;

b) The name of the individual making the request;

c) The mode in which the request is made, i.e. email, phone call;

d) Type of proof of the identity of the individual making the request;

e) Type of proof, if any, supporting the correction or omission of personal data;

f) The date which the DPO accede or decline the request;

g) The reasons and reasonable steps taken should the request be declined;

h) Steps taken to determine if personal data had been provided to another organisation(s) within twelve (12) months and if notification to the organisation(s) is necessary;

i) Notification of correction received from another organisation, including reason(s) for not making the correction, if any; and

j) Legal advice obtained, if any.

9 ACCURACY OF PERSONAL DATA

9.1 General Principles

9.1.1 TOMO shall make reasonable effort to ensure all personal data collected is accurate and complete.

9.1.2 To ensure accurate data collection and input, all staff shall:

a) Act diligently and conscientiously in collecting personal data from any individual in the course of their work with TOMO:

b) Verify information provided by an individual, to the extent possible;

c) Take steps to ensure data input into electronic files are complete and accurate, i.e. verify the accuracy and completeness by an independent personnel; and

d) Seek assistance or guidance from their supervisor / DPO in any instance where they believe that an individual does not provide to TOMO:

i) Information that is accurate; and/or

ii) Information that is complete, in the context to the purpose for which it is provided for.

10 PROTECTION OF PERSONAL DATA

10.1 General Principles

10.1.1 TOMO shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

10.1.2 The following PDPC general guides shall be referred to for more information on the protection of personal data:

a) Guide to Securing Personal Data in Electronic Medium (Updated on 20 January 2017);

b) Guide to Disposal of Personal Data on Physical Medium (Updated on 20 January 2017); and

c) Guide to Printing Processes for Organisations (Published on 3 May 2018).

10.1.3 The DPO shall maintain TOMO's personal data inventory map to track the types of personal data collected, used and disclosed by TOMO.

*Refer to **Appendix 8** for the Personal Data Inventory Map Template*

10.2 Physical Security

10.2.1 TOMO shall undertake, but not limited to, the following steps to protect the personal data held:

a) Marking electronic, paper files and documents as 'Confidential'

i) Staff should ensure that the files or documents which personal data is recorded is clearly marked as 'Confidential'.

b) Restrict access to personal data

i) Staff should only have access to the personal data, for the purpose of performing their roles and responsibilities with TOMO; and

ii) Staff should not allow other staff to have access to the personal data, except to the extent in which the staff needs to carry out their roles and responsibilities.

c) Destruction of paper files

i) Staff should ensure that any paper document containing personal data are disposed securely, i.e. shredding of the paper document;

ii) DPO shall ensure that a qualified vendor is appointed for disposal of documents, containing personal data, securely, if documents could not be shredded at TOMO premises; and

iii) Staff should ensure that any paper document containing personal data are not retained so that the blank page of the document may be used.

d) No copying of personal data or use other than by TOMO

i) All staff shall be prohibited from:

- Making any copy, in any form, of personal data about any individual; and / or
- Providing any personal data about any individual to any person.

Except for the sole purpose of performing their role with TOMO.

e) Personal data printed through the common printer

i) All staff have a responsibility to minimise the incidence of any document containing personal data being viewed by a person who is not entitled to have access to that personal data. All staff, who are printing any file that contains or may contain personal data, shall retrieves the output from the printer immediately.

f) Hardcopy / paper files

i) The following files containing personal data shall be kept in locked cabinets in which only the authorised staff, holds the key.

- Members files;
- Staff personnel files;
- Donor records; and
- Volunteer records.

g) Clean desk policy

i) All staff shall ensure that:

- All hardcopy / paper files are placed in locked cabinets at the end of each working day; and
- Any hardcopy / paper files containing personal data is not left unattended in clear view while the staff if temporarily away, i.e. lunch break.

h) Keys / Access Cards

i) Office Manager shall ensure that all keys / access cards to TOMO's offices are returned upon the last day of service of the resigned staff.

10.3 Logical Security

10.3.1 DPO shall have the oversight role in ensuring that the personal data held electronically are secured in the information technology systems used.

10.3.2 DPO shall ensure that reasonable measures are in place to prevent unauthorised access to the information technology systems operated by TOMO.

10.3.3 All staff shall have the responsibility to ensure that electronic personal data are secured, including but not limited to the following:

a) Files which contained personal data are encrypted and/or password protected; and

b) Transmissions of files containing personal data are encrypted and/or password protected.

10.3.4 The DPO shall ensure that:

a) All servers or other hardware that are used to store personal data are password protected, and the password is held by the IT Administrator or anyone who is authorised by the CEO.

b) All PCs, laptops or any hardware that may be used to access personal data are protected by a log-on password;

c) All PCs and laptops that may be used to access personal data shall require a screensaver password if not used for more than five (5) minutes;

d) Access credentials of an individual are terminated immediately upon last day of service;

e) All PCs, laptops, servers and any other hardware shall be disposed by an authorised vendor, who shall provide a certificate of destruction, upon completion of disposal.

10.4 Bring Your Own Device

10.4.1 TOMO grants its staff the privilege of using smartphones and tablets of their choosing at work for their convenience, which may involve handling personal data.

10.4.2 Staff must ensure that personal devices, which are used to access personal data, are password protected.

10.4.3 If the staff suspects a data breach and/or leakage from its personal device, it shall be reported to the DPO immediately.

10.5 Records Disposal

10.5.1 DPO shall ensure that all hardcopy records that are disposed are properly accounted for. The disposal process shall be approved by the CEO.

10.5.2 Controls shall be put in place to preserve the integrity of the record disposal process.

10.5.3 All electronic records must be deleted from the system at the end of the retention period.

10.5.4 IT equipment must be properly disposed by an authorised outsourced agency or through physical destruction of the equipment.

11 RETENTION OF PERSONAL DATA

11.1 General Principles

11.1.1 TOMO shall cease to retain its documents, both electronic and hardcopy, containing personal data as soon as it is reasonable to assume:

a) The purpose for which that personal data was collected is no longer being served by retention of personal data; or

b) Retention is no longer necessary for legal or business purposes.

11.2 Records Retention Period

11.2.1 All records containing personal data shall be kept for the period, as specified:

Categories of personal data	Retention Period
Rejected job applicant records	Immediate
Potential job applicant records	Within the probation period of a new staff
Resigned staff records	Six (6) years
Retired Board and Sub-Committee member records	
Member records	
Community Member records	
Donor records	
Volunteer records	

12 COMPLAINTS HANDLING

12.1 Receipt of Complaint

12.1.1 All complaints regarding the collection, use or disclosure of personal data shall be referred to the DPO immediately.

12.1.2 DPO shall make reasonable efforts to obtain sufficient information from the individual to investigate the complaint, such as:

a) The type of action or lack of action that gives rise to the individual's concern;

b) Whether it is an isolated incident. If it is an isolated incident, the time of occurrence; and

c) A copy of any relevant correspondence held by the individual.

12.2 Resolving of Complaint

12.2.1 DPO should investigate immediately and reply within five (5) working days to the individual, advising the individual on the status of the outcome or investigation.

12.2.2 DPO shall ensure all investigations are completed within two (2) weeks.

12.2.3 All communications to the individual shall be in writing, either through email or letter.

12.3 Follow-up Actions

12.3.1 DPO shall review the complaints received periodically and determine if further actions are required to be taken to remedy the situation. This could include reviewing of current practices, documents or additional training for staff is required.

12.4 Records

12.4.1 The DPO shall maintain records of the complaints received, with the following details:

a) The date which TOMO received the complaint;

b) The name of the individual making the complaint;

c) Details of the complaint;

d) The mode in which the complaint is made, i.e. email, phone call;

e) Steps taken by the DPO to investigate the complaint;

f) The outcome of the complaint;

g) The response given to the individual by the DPO; and

h) If the complaint is not resolved to the satisfaction of the individual, the reasons provided by the DPO for the outcome.

13 MANAGING DATA BREACHES

13.1 General Principles

13.1.1 A data breach refers to an incident exposing personal data in TOMO possession or under its control to the risks of unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.

13.1.2 Data breaches often lead to financial losses and a loss of stakeholders' (e.g. donors, members, volunteers) trust for TOMO. In addition, individuals whose personal data have been compromised could be at risk of harm or adverse impact if they do not take steps to protect themselves.

13.1.3 Data breaches could occur in the following possible ways:

a) Malicious activities

i) Hacking incidents / illegal access to databases;

ii) Theft of laptops, data storage devices or paper records; or

iii) Scams that trick organisations into releasing personal data of individuals.

b) Human error

i) Loss of laptops, data storage devices or paper records;

ii) Sending personal data to a wrong email or physical address or disclosing to a wrong recipient;

iii) Unauthorised access of disclosure of personal data by staff; or

iv) Improper disposal of personal data, i.e. hard disk, storage media or paper documents containing personal data sold or discarded before data is properly deleted.

c) Computer system error

i) Errors or bugs in the programming code of websites, databases and other software which may be exploited to gain access to personal data stored on computer systems.

13.2 Managing Data Breach

13.2.1 TOMO has developed a Data Breach Management Plan to handle data breaches.

13.2.2 Staff should follow the procedures set out in the Data Breach Management Plan, wherever required.

14 LIST OF APPENDICES

Appendices	Description	Template
1	Training and Communications Plan	Appendix 1 - Training & Communications Pl
2	DPIA Report Template	Appendix 2 - DPIA Report Template.xlsx
3	DPIA Log	Appendix 3 - DPIA Log.docx
4	Access Request Form	Appendix 4 - Access Request Form.docx
5	Acknowledgement of Personal Data Received for an Access Request Form	Appendix 5 - Acknowledgement of
6	Correction Request Form	Appendix 6 - Correction Request Fc
7	Acknowledgement of Personal Data Correction Form	Appendix 7 - Acknowledgement of
8	Personal Data Inventory Map Template	Appendix 8 - Personal Data Invento