A Privacy Management Programme (“**PMP**”) is not a requirement under the Personal Data (Privacy) Ordinance (“**PDPO**”). However, a PMP serves as a strategic framework to assist organisations in building a robust privacy infrastructure and setting policies to facilitate compliance with the requirements under the PDPO. NGOs may use this template as a guide to develop their own PMP manual and adjust the content depending on their own circumstances. An organisation should follow its PMP manual when governing the collection, processing, maintenance and disposal of personal data.

This guide does not represent a code of practice under section 12 of the PDPO or a guidance note which provides direct guidance for compliance with specific provisions of the PDPO. This is a reference guide for a PMP manual to reflect some of the best practices advocated by the Privacy Commissioner for Personal Data, Hong Kong (“**Privacy Commissioner**”) instead of prescriptive obligations to be met by organisations.

**Acknowledgement**

This template is modelled on the “General Reference Guide – PMP Manual” issued by the Privacy Commissioner (<https://www.pcpd.org.hk/misc/files/grg_private_sector.pdf>).

**Disclaimer**

The information provided in this PMP manual is for general reference only. It does not serve as an exhaustive guide to the application of the PDPO. For a complete and definitive statement of law, direct reference should be made to the latest version of the PDPO itself. PILnet makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information herein. PILnet does not accept responsibility or liability for any loss or damage suffered or incurred by you or any other person or entity however caused relating in any way to this PMP manual, without limitation, the information contained in or provided in connection with it, any errors or omissions from it however caused. PILnet does not accept any responsibility for any matters arising out of this PMP manual. If you need further information or legal advice in relation to this PMP manual, please contact PILnet at hkprobono@pilnet.org or +852 6106 0892 for assistance.

**[*Logo of the NGO*]**

**Privacy Management Programme Manual**

**of**

**[*Name of NGO*]**

**TABLE OF CONTENTS**

[**1.** **INTRODUCTION TO THE PRIVACY MANAGEMENT PROGRAMME** 4](#_Toc73631633)

[**2.**  **OVERVIEW OF THE PERSONAL DATA (PRIVACY) ORDINANCE** 5](#_Toc73631634)

[**2.1** **Legislative Background** 5](#_Toc73631635)

[**2.2** **Key Definitions under the PDPO** 5](#_Toc73631636)

[**2.3** **Data Protection Principles** 7](#_Toc73631637)

[**2.4** **Contravention of the PDPO** 8](#_Toc73631638)

[**3.**  **THE PMP OF [*FULL NAME OF NGO*]** 13](#_Toc73631639)

[**3.1** **Organisational Commitment** 13](#_Toc73631640)

[**3.1.1** **Roles and Responsibilities of the Data Protection Officer and Other Officers Assisting in the Implementation of PMP** 13](#_Toc73631641)

[**3.1.2** **Reporting Mechanism** 16](#_Toc73631642)

[**3.2** **Programme Controls** 16](#_Toc73631643)

[**3.2.1** **Personal Data Inventory** 16](#_Toc73631644)

[**3.2.2** **Policies on Personal Data Handling** 18](#_Toc73631645)

[**3.2.3** **Direct Marketing** 22](#_Toc73631646)

[**3.2.4** **Risk Assessment Tools** 23](#_Toc73631647)

[**3.2.5** **Training and Education for Staff** 25](#_Toc73631648)

[**3.2.6** **Data Breach Handling** 26](#_Toc73631649)

[**3.2.7** **Data Processor Management** 31](#_Toc73631650)

[**3.2.8** **Communication** 32](#_Toc73631651)

[**3.2.9** **Social Media Policy** 32](#_Toc73631652)

[**3.2.10** **Job Applicants Data Handling Policy** 34](#_Toc73631653)

[**3.3** **Ongoing Assessment and Revision** 35](#_Toc73631654)

[**3.3.1** **Development of an Oversight and Review Plan** 35](#_Toc73631655)

[**3.3.2** **Review of PMP’s Effectiveness** 36](#_Toc73631656)

**Annex A Sample of Personal Information Collection Statement**

**Annex B Data Access and Correction Policy**

**Annex C Data Access Request Form**

**Annex D Personal Data Correction Request Form**

**Annex E Complaints and Enquiries Handling Policy**

**Annex F Sample of Personal Data Inventory**

**Annex G Sample of Risk Assessment Questionnaire**

**Annex H Sample of Privacy Impact Assessment Questionnaire**

**Annex I Data Breach Information Sheet**

**Annex J Data Processor Review Checklist**

**Annex K Sample of Privacy Policy Statement**

**Annex L Differences between NGOs with more resources and NGOs with limited resources**

# **1. INTRODUCTION TO THE PRIVACY MANAGEMENT PROGRAMME**

The Privacy Commissioner for Personal Data, Hong Kong (the “**PCPD**” or the “**Privacy Commissioner**”) advocates that organisational data users should embrace personal data privacy protection as part of their corporate governance responsibilities and apply it as a business imperative throughout the organisation, covering business practices, operational procedures, service design, physical architectures and network infrastructure.

A Privacy Management Programme (“**PMP**”) is a strategic framework, which assists organisations to build robust privacy infrastructures supported by effective on-going review and monitoring processes. It also facilitates organisations to comply with the requirements under the Personal Data (Privacy) Ordinance of Hong Kong (Cap.486) (the “**PDPO**”). In February 2014, the PCPD issued the “Privacy Management Programme: A Best Practice Guide”, which was subsequently revised in August 2018 and March 2019, outlining good approaches for developing a PMP.[[1]](#footnote-1)

This PMP Manual serves as a reference guide for [*Name of NGO*] (“**[\_\_\_]**”) to develop and implement its PMP. This PMP Manual outlines the policies, practices, requirements and guidance relating to the handling of personal data at [\_\_\_\_].

**Enquiries**

Any enquiries regarding (i) this PMP Manual; (ii) the implementation of the PMP at [\_\_\_\_]; and (iii) the handling of personal data at [\_\_\_\_] should be addressed to the Data Protection Officer of [\_\_\_\_] at [*email address*].

# **2. OVERVIEW OF THE PERSONAL DATA (PRIVACY) ORDINANCE**

## **2.1 Legislative Background**

The PDPO was enacted in 1995 and amended in 2012 and 2021. The objective of the PDPO is to protect the privacy of individuals in relation to personal data.

## **2.2 Key Definitions under the PDPO**

**Personal Data[[2]](#footnote-2)**

*Personal data* means any data –

(a) relating directly or indirectly to a living individual;

(b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and

(c) in a form in which access to or processing of the data is practicable.

Examples of personal data collected, used and/or processed at [\_\_\_\_] include: ***[Note: NGO to amend/supplement as appropriate]***

* full name;
* date and place of birth;
* contact details such as e-mail address, mailing and residential address, telephone numbers and fax number;
* information for verification of identity, including identification type and number (such as Hong Kong Identity Card or passport number) and other related information (such as membership numbers, if applicable);
* employment-related record (e.g., resume, performance appraisal report, conduct and discipline, training and developments, leave files, records related to salary and other fringe benefits, etc.);
* billing information, including bank account and credit card information and details;
* demographic information, including age, gender, nationality, marital status, educational and professional background, community services and extra-curricular activities;
* areas of interest;
* image and voice, including photographs, video or audio recordings; and
* spouse and family information, including any of their above information.

**Data Subject2**

A *data subject* refers to the living individual who is the subject of the personal data concerned. A deceased person is not a data subject under the PDPO.

For NGOs, data subjects are people from whom the NGOs obtain personal data, which may include participants in services or activities held by the NGO, staff, job applicants and social workers.

**Data User2 and Data Processor[[3]](#footnote-3)**

A *data user* is a person or an organisation that either alone or jointly or in common with other persons or organisations, controls the collection, holding, processing or use of personal data. NGOs, as organisations which collect and use individuals’ personal data, are data users.

A *data processor* is a person who –

(a) processes personal data on behalf of another person; and

(b) does not process the data for any of the person’s own purposes.

A data user is liable as the principal for the wrongful act of its authorised data processor. For NGOs, data processors are usually third party contractors engaged by the NGOs to outsource work involving personal data processing. They may include, among others, providers of IT processing and marketing companies which carry out surveys on behalf of the NGOs.

**Personal Identifier2**

*Personal identifier* means an identifier –

(a) that is assigned to an individual by a data user for the purpose of the operations of the user; and

(b) that uniquely identifies an individual in relation to the data user,

but does not include an individual’s name used to identify that individual.

**Direct Marketing, Direct Marketing Means, Marketing Subject, Permitted Class of Marketing Subjects and Consent[[4]](#footnote-4)**

*Direct marketing* means –

(a) the offering, or advertising of the availability, of goods, facilities or services; or

(b) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes,

through direct marketing means;

*Direct marketing means* means –

(a) sending information or goods, addressed to specific persons by name, mail, fax, electronic mail or other means of communication; or

(b) making telephone calls to specific persons.

*Marketing subject*, in relation to direct marketing, means –

(a) any goods, facility or service offered, or the availability of which is advertised; or

(b) any purpose for which donations or contributions are solicited.

*Permitted class of marketing* *subjects* means a class of marketing subjects in relation to which a data subject has provided his/her consent to the data user for the use or provision of his/her personal data in direct marketing.

*Consent*, in relation to a use of personal data in direct marketing or a provision of personal data for use in direct marketing, includes an indication of no objection to the use or provision.

## **2.3 Data Protection Principles**

The six data protection principles (“**DPPs**”) set out in Schedule 1 to the PDPO represent the normative core of the PDPO and cover the life cycle of a piece of personal data.

**DPP1 – Data Collection Principle**

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function or an activity of the data user. Data collected should be necessary but not excessive.

Where personal data are collected from data subjects directly, all practicable steps should be taken to notify the data subjects on or before collection of the data of the purpose of data collection, and the classes of persons to whom the data may be transferred. The best practice to fulfil these requirements is to provide data subjects with a Personal Information Collection Statement (“**PICS**”). For a sample of a PICS, please refer to **Annex A** of this PMP Manual. For guidance on preparing a PICS, please refer to “Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement” issued by the PCPD.[[5]](#footnote-5)

**DPP2 – Data Accuracy and Retention Principle**

All practicable steps should be taken to ensure that personal data are accurate and should not be kept for a period longer than is necessary to fulfil the purpose for which it is used, i.e. personal data should be disposed of when they are no longer required for the purpose for which they were originally collected.

**DPP3 – Data Use Principle**

Personal data should only be used for the purpose for which the data are collected or for a directly related purpose, unless the data user obtains from the data subject voluntary and explicit consent to use the data for a new purpose.

**DPP4 – Data Security Principle**

A data user needs to take all practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

**DPP5 – Openness Principle**

A data user should take all practicable steps to make known to the public its personal data policies and practices, kinds of personal data it holds and the purposes for which the data are or are to be used.

**DPP6 – Data Access and Correction Principle**

A data subject has the right to (i) request access to his/her own personal data held by a data user, and (ii) request the correction of the personal data supplied in a data access request if the data are inaccurate. Please refer to **Annex B** of this PMP Manual for the Data Access and Correction Policy of [\_\_\_\_].

**Exemption**

In general, the above six DPPs should be followed. However, there are specific cases where the PDPO provides exemption. For example, personal data held for the purpose of prevention and detection of a crime may be exempt from the provisions in respect of data access request (DPP6) and restrictions on the use of personal data (DPP3). For details of exemptions granted, please refer to Part 8 of the PDPO.

## **2.4 Contravention of the PDPO**

**Contravention of the DPPs**

Contravention of the DPPs does not directly constitute a criminal offence. The Privacy Commissioner may serve an enforcement notice to direct the data user to remedy the contravention.

***Offences relating to Enforcement Notices***

However, contravention of an enforcement notice is an offence and the data user is liable –

(a) on a first conviction –

i. to a fine at level 5 (i.e. $50,000) and to imprisonment for 2 years; and

ii. if the offence continues after the conviction, to a daily penalty of $1,000; and

(b) on a second or subsequent conviction –

i. to a fine at level 6 (i.e. $100,000) and to imprisonment for 2 years; and

ii. if the offence continues after the conviction, to a daily penalty of $2,000.[[6]](#footnote-6)

Please note that depending on the circumstances, the penalty is a fine and/or imprisonment up to the amounts/length of time stated above. It is a defence for the data user charged to show that the data user exercised all due diligence to comply with the enforcement notice.[[7]](#footnote-7)

**Contravention of the provisions under the PDPO**

Contraventions of certain provisions under the PDPO are criminal offences. Examples include unauthorised disclosure of personal data without consent of a data user or a data subject, non-compliance with data access requests or data correction requests, use of personal data in direct marketing activities, failure to erase personal data no longer required and failure to comply with requirements of the Privacy Commissioner. The relevant provisions are elaborated below.

• ***Unauthorised disclosure of personal data without consent from data users***

A person commits an offence if he/she discloses any personal data of a data subject obtained from a data user without the data user’s consent, with an intent –

(a) to obtain gain in money or other property, whether for the benefit of the person or another person; or

(b) to cause loss in money or other property to the data subject.[[8]](#footnote-8)

The maximum penalty of committing the above offences is a fine of $1 million and imprisonment for 5 years.[[9]](#footnote-9)

• ***Unauthorised disclosure of personal data without consent from data subjects***

A person also commits an offence if he/she discloses any personal data of a data subject without the data subject’s consent –

(a) with an intent to cause any specified harm to the data subject or any family member of the data subject; or

(b) being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject.[[10]](#footnote-10)

The maximum penalty of committing the above offences is a fine at level 6 (i.e. $100,000) and imprisonment for 2 years.[[11]](#footnote-11)

A person also commits an offence if –

(a) he/she discloses any personal data of a data subject without the relevant consent of the data subject –

(i) with an intent to cause any specified harm to the data subject or any family member of the data subject; or

(ii) being reckless as to whether any specified harm would be, or would likely be, caused to the data subject or any family member of the data subject; and

(b) the disclosure causes any specified harm to the data subject or any family member of the data subject. [[12]](#footnote-12)

The maximum penalty of committing the above offences is a fine of $1 million and imprisonment for 5 years.[[13]](#footnote-13)

• ***Non-compliance with data access requests or data correction requests***

Upon receiving a data access request, a data user is required to supply a copy of the requested data to the requestor within 40 calendar (not working) days, unless under the circumstances allowed by the PDPO.[[14]](#footnote-14)

A data subject is entitled to make a data correction request after being supplied with his/her personal data by a data user pursuant to a data access request.

Upon receiving a data correction request, the data user should make the necessary correction and supply a copy of the corrected data to the requestor within 40 calendar (not working) days, unless under the circumstances allowed by the PDPO.[[15]](#footnote-15)

Failure to handle a data access request or a data correction request in accordance with the requirements under the PDPO without reasonable excuse may constitute an offence and render the offender liable on conviction to a fine at level 3, i.e. $10,000.[[16]](#footnote-16)

• ***Use of personal data in direct marketing activities in contravention of Part 6A of the PDPO[[17]](#footnote-17)***

Under the PDPO, a data user is required to notify the data subjects and obtain their consents before using their personal data for direct marketing purposes, or transferring such data to a third party for direct marketing purposes. A data user is also required to comply with a data subject’s request, if so made, to cease to use his/her personal data in direct marketing.

Contravention of the above-mentioned direct marketing requirements is punishable by a fine of up to $500,000 and imprisonment for 3 years. If the personal data are provided to a third party for its use in direct marketing in exchange for gain, the maximum penalty is a fine of $1 million and imprisonment for 5 years. For details of the direct marketing requirements under the PDPO, please refer to the “New Guidance on Direct Marketing” issued by the PCPD.[[18]](#footnote-18)

• ***Failure to erase personal data no longer required***

Section 26of the PDPO provides that a data user must take all practicable steps to erase personal data held when the data are no longer required for the purpose for which they were used, unless any such erasure is prohibited under any law or it is in the public interest not to have the data erased.

Contravention of section 26 of the PDPO is an offence and the offender is liable on conviction to a fine at level 3, i.e. $10,000.[[19]](#footnote-19)

• ***Failure to comply with requirements of the Privacy Commissioner[[20]](#footnote-20)***

When the Privacy Commissioner or a person designated by the Privacy Commissioner performs his/her functions or exercises his/her powers in relation to inspection and investigation under the PDPO, a person commits an offence if he/she:

(a) without lawful excuse, obstructs, hinders or resists the Privacy Commissioner or the person designated by the Privacy Commissioner in performing such functions or exercising such powers of the Privacy Commissioner;

(b) without lawful excuse, fails to comply with any lawful requirement of the Privacy Commissioner or the person designated by the Privacy Commissioner; or

(c) provides statements which the person knows to be false or does not believe to be true or knowingly misleads the Privacy Commissioner or the person designated by the Privacy Commissioner.

The maximum penalty of committing the stated offence is a fine at level 3, i.e. $10,000, and imprisonment for 6 months.

• ***Failure to comply with requirements of the Privacy Commissioner with respect to offences under Section 64 of the PDPO[[21]](#footnote-21)***

The PDPO empowers the Privacy Commissioner to conduct criminal investigations, issue cessation notices, and institute prosecutions for doxxing and related offences.

When the Privacy Commissioner performs his/her functions or exercises his/her powers to require materials and assistance under the PDPO for the purpose of their conduct of investigations into doxxing and related offences, a person commits an offence if he/she fails to comply with a requirement of a notice given to him/her by the Privacy Commissioner.[[22]](#footnote-22)

The maximum penalty of committing the stated offence is a fine of $200,000 and imprisonment for 1 year.

For more information regarding doxxing offences and related criminal liabilities, please refer to “Personal Data (Privacy) (Amendment) Ordinance 2021 Implementation Guideline” issued by the PCPD.[[23]](#footnote-23)

# **3. THE PMP OF [*FULL NAME OF NGO*]**

This PMP consists of three parts. Part 1 outlines [\_\_\_\_]’s organisational commitment to have an internal governance structure in place that fosters a culture respectful of privacy. Part 2 discusses the programme controls, which are the components required for an effective governance structure. Part 3 discusses how to maintain and improve a PMP on an ongoing basis.

## **3.1 Organisational Commitment**

### **3.1.1 Roles and Responsibilities of the Data Protection Officer and Other Officers Assisting in the Implementation of PMP**

[\*] has been appointed as the Data Protection Officer and [\*] has been appointed as the Personal Data Privacy Officer of [\_\_\_\_].

***[Note: NGO to review the responsibilities of the different roles and amend as appropriate. Two positions are stated in this template to share the responsibilities.***

***For NGOs which have limited resources and can only have one person designated for data privacy issues, the designated person should be appointed as the Data Protection Officer and handle all responsibilities mentioned below including handling of privacy complaints/enquiries and data access/correction requests. For NGOs with more resources/manpower, please consider assigning additional responsible staff to implement and manage this PMP, by including the following in this PMP.*]**

[The following staff members will also assist in the implementation and management of the PMP:-

|  |  |  |
| --- | --- | --- |
| **Role** | **Department** | **Responsible Staff** |
| Departmental Coordinator | [Administration] | [\_\_\_] |
| [Information Technology] | [\_\_\_] |
| [Corporate Communications] | [\_\_\_] |
| [Legal] | [\_\_\_] |
| [Marketing] | [\_\_\_] |

]

**Data Protection Officer**

The Data Protection Officer should manage the implementation of the PMP and facilitate [\_\_\_\_]’s compliance with the PDPO. He/she should represent [\_\_\_\_] in the event of an enquiry, an inspection or an investigation by the Privacy Commissioner and/or other law enforcement agencies (e.g. the Hong Kong Police Force). The Data Protection Officer’s responsibilities include:

(i) establishing and implementing the PMP programme controls, in particular –

• keeping a record of [\_\_\_\_]’s **personal data inventory**; initiating and monitoring the annual personal data inventory review exercise (for details of the personal data inventory, please refer to Section 3.2.1 below);

• initiating the **periodic risk assessment** and reviewing the completed risk assessment questionnaire (for details of periodic risk assessment, please refer to Section 3.2.4 below);

• monitoring, reviewing and conducting **privacy impact assessments** in [\_\_\_\_] (for details of privacy impact assessments, please refer to Section 3.2.4 below);

• carrying out **training and education** within [\_\_\_\_] and promoting staff awareness on privacy protection by circulating updates on data privacy policies, guidelines and other privacy-related information (for details of the training and education plan, please refer to Section 3.2.5 below);

• coordinating and monitoring the handling of **data breach incidents**; providing advice on conducting investigations and post-incident reviews (for details of data breach handling, please refer to Section 3.2.6 below);

• providing advice on **data processor management** and carrying out data processor management review (for details of data processor management, please refer to Section 3.2.7 below);

• circulating the PMP Manual and other prevailing data privacy policies and guidelines to staff on a half-yearly basis (for details of communication of personal data policies and practices, please refer to Section 3.2.8 below); and

• monitoring, reviewing and providing advice on the preparation of PICS before a PICS is presented to an individual for collecting his/her personal data (for details on a sample of a PICS, please refer to **Annex A** of this PMP Manual);

(ii) reviewing the effectiveness of the PMP and revising the programme controls where necessary, in particular –

• preparing [\_\_\_\_]’s **oversight and review plan for the PMP** and carrying out reviews according to the oversight and review plan (for details of the oversight and review plan, please refer to Section 3.3.1 below); and

• conducting **annual review of the effectiveness of the PMP**; revising and updating the PMP and the relevant programme controls based on the assessment result (for details of the review checklist, please refer to Section 3.3.2 below).

**Personal Data Privacy Officer**

The Personal Data Privacy Officer should assist the Data Protection Officer in performing his/her tasks regarding the implementation of the PMP in [\_\_\_\_]. His/her responsibilities include:

(i) handling **privacy complaints or enquiries** to [\_\_\_\_] in relation to personal data or the PMP (for details of complaints and enquiries handling, please refer to **Annex E** of this PMP Manual);

(ii) handling **data access or correction requests** made to [\_\_\_\_] under the PDPO (for the Data Access Request Form, please refer to **Annex C** of this PMP Manual; for a sample of the Personal Data Correction Request Form, please refer to **Annex D** of this PMP Manual); and

(iii) assisting the Data Protection Officer in implementing the PMP programme controls as described above and carrying out ongoing assessment and revision of the PMP.

**[*Note: For those NGOs with more resources/manpower to designate departmental coordinators, please consider specifying the following responsibilities.*]**

[**Departmental Coordinators**

The Departmental Coordinators should manage the implementation of the PMP within their respective departments, and represent their respective departments to communicate with the Data Protection Officer for matters related to the PMP. Their responsibilities include:

(i) conducting annual review of the **personal data inventory** of their respective departments and submitting the updated personal data inventory to the Data Protection Officer (for details of the personal data inventory, please refer to Section 3.2.1 below);

(ii) carrying out **periodic risk assessments** within their respective departments by completing the **risk assessment questionnaire**, and submitting the questionnaire result to the Data Protection Officer (for details of periodic risk assessment, please refer to Section 3.2.4 below, and for a sample of the risk assessment questionnaire, please refer to **Annex G** of this PMP Manual);

(iii) conducting **data processors management review** for their respective departments by completing the **Data Processor Review Checklist** and submitting the completed checklist to the Data Protection Officer (for details of the data processor review checklist, please refer to **Annex J** of this PMP Manual);

(iv) assisting the Data Protection Officer in carrying out **ongoing assessment and revision of data privacy policies and practices** (for details of ongoing assessment and revision, please refer to Section 3.3 below.]

**[*Note: NGOs can determine the responsibilities of the Data Protection Officer, Personal Data Privacy Officer and Departmental Coordinators depending on their actual circumstances.*]**

### **3.1.2 Reporting Mechanism**

With regard to the roles and responsibilities to assist in the implementation of the PMP as described, [each of the Department Coordinators and ]the Personal Data Privacy Officer will report to the Data Protection Officer, who reports directly to the [board] of [\_\_\_\_]. The adoption of and any amendments to this PMP Manual and the PICS require approval of the [board] of [\_\_\_\_]. ***[Note: NGO to confirm/determine the highest authority]***

## **3.2 Programme Controls**

Programme controls are measures that assist [\_\_\_\_] to develop a PMP. Developing these controls can ensure that [\_\_\_\_] is compliant with the PDPO.

### **3.2.1 Personal Data Inventory**

[\_\_\_\_] collects, holds, processes and uses different types of personal data. Examples of categories and types of personal data collected, held, processed and/or used at [\_\_\_\_] include, but are not limited to, the following: ***[Note: NGO to review and amend as appropriate]***

|  |  |
| --- | --- |
| **Category of Personal Data** | **Type of Personal Data** |
|  |  |
| [Personnel-related records] | [e.g. Leave files, performance appraisals, HKID numbers, contact information, records on salaries and allowances, training and development, benefits, conduct and discipline, etc.] |
| [Member/non-member records] | [e.g. Membership records, transaction records, contact information, demographic information, credit card information, etc.] |
| [General administrative / operational records] | [e.g. Public enquiries and complaints, procurement matters, closed-circuit television (i.e. CCTV) records, etc.] |

**[*Note: NGOs may adjust the categories above in light of the actual circumstances.*]**

[\_\_\_\_] should be clear about:

* what kinds of personal data it holds and where the data are held and document its assessment; and
* why it is collecting, using or disclosing personal data and document the reasons.

The Data Protection Officer is responsible for maintaining a personal data inventory, which covers relevant details of all personal data [\_\_\_\_] holds. A sample of the personal data inventory is included in **Annex F** of this PMP Manual. [\_\_\_\_] should update its personal data inventory annually to ensure that all the personal data it holds are well recorded in the personal data inventory.

**[*Note: NGOs with more resources/manpower to designate Departmental Coordinators may consider setting forth the following Steps 1-5 governing the procedure for reviewing and updating the personal data inventory.*]**

[**Step 1 – Initiate the review exercise (Action by Data Protection Officer)**

The Data Protection Officer should initiate the exercise by requesting Departmental Coordinators to review and update the entries in the personal data inventory under the purviews of their respective departments.

**Step 2 – Review the personal data inventory (Action by Departmental Coordinators)**

Upon receipt of a request from the Data Protection Officer, Departmental Coordinators should conduct the annual review of the personal data inventory for their respective departments with inputs from other staff members of their departments, and update the personal data inventory as appropriate and keep track of retention period of the personal data. Departmental Coordinators should ensure that all types of records containing personal data held by their respective departments are included in the personal data inventory.

**Step 3 – Submit the updated personal data inventory to the Data Protection Officer (Action by Departmental Coordinators)**

Departmental Coordinators should submit the updated personal data inventory for their respective departments to the Data Protection Officer for review and consolidation.

**Step 4 – Review and finalise the updated personal data inventory (Action by Data Protection Officer)**

The Data Protection Officer should review the updated personal data inventory submitted by the Departmental Coordinators and seek clarification or further information from the Departmental Coordinators when necessary, to ensure information contained in the personal data inventory is clear. When no further clarification or information is required, the updated personal data inventory can be finalised.

**Step 5 – File the updated personal data inventory (Action by Data Protection Officer)**

Once the updated personal data inventory is finalised, the Data Protection Officer should file the updated personal data inventory for record. The Data Protection Officer should ensure that the updated personal data inventory covers all personal data held by [\_\_\_].]

### **3.2.2 Policies on Personal Data Handling**

[\_\_\_\_] has established various policies and guidelines to fulfil requirements under the six DPPs of the PDPO:

**DPP1 – Collection of Personal Data**

When collecting personal data, [\_\_\_\_] must satisfy itself that:

(i) the purposes for which the data are collected are lawful and directly related to a function or activity of [\_\_\_\_];

(ii) the manner of collection is lawful and fair in the circumstances of the case; and

(iii) the personal data collected are necessary but not excessive for the purpose(s) for which they are collected.

On or before the collection of personal data from an individual (i.e. the data subject), [\_\_\_\_] should always provide the data subject with a PICS in writing.

**DPP2 – Accuracy and Retention of Personal Data**

Personal data collected and maintained by [\_\_\_\_] should be as accurate, complete, and up-to-date as is necessary for the purpose for which they are to be used.

[\_\_\_\_] should maintain an up-to-date personal data inventory to monitor and keep track of the retention period of records that contain personal data. Please refer to **Annex F** of this PMP Manual for a personal data inventory which contains information on retention period of data.

[Departmental Coordinators should arrange to dispose of records containing personal data in accordance with [\_\_\_\_]’s records management guidelines and procedures, where appropriate.] **[*Note: applicable to NGOs with more resources/manpower to designate Departmental Coordinators.*]**

Personal data in electronic records should be deleted when there is no longer an operational need to retain the data.

If [\_\_\_] engages a data processor, [\_\_\_] must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary. For details of data processor management, please refer to Section 3.2.7 of this PMP Manual.

**DPP3 - Use of Personal Data**

All personal data collected should be used solely for the purposes which are directly related to the discharge of [\_\_\_\_]’s functions. Personal data collected may only be transferred to third parties during the discharge of [\_\_\_\_]’s functions when necessary. Relevant personal data may also be disclosed to other entities, which are authorised to receive information for the purposes of law enforcement, prosecution or review of decisions. Data subjects must be informed of the possible transferees of their personal data when their personal data are collected.

If personal data are to be used for a purpose other than the purposes for which the data are collected, express prior consent in writing should be sought from the data subject concerned. In seeking the data subject’s consent, all practicable steps must be taken to ensure that (i) information provided to the data subject is clearly understandable and readable; and (ii) the data subject is informed that he/she is entitled to withhold or withdraw his/her consent subsequently by giving notice in writing.

**DPP4 – Security of Personal Data**

[\_\_\_\_] takes practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use. All staff handling personal data should strictly observe relevant security guidelines and regulations of [\_\_\_\_], and implement, where appropriate, the security measures listed below to safeguard personal data. Examples include:

(i) restriction of access to personal data on a “need-to-know” basis;

(ii) regular review and enhancement of security measures for protection of personal data in the servers, user computers, BYOD (i.e. Bring Your Own Device) and transmission of electronic messages, etc.;

(iii) regular change of passwords for IT facilities, accounting and personnel systems, etc.;

(iv) encryption of all backup storages that are to be transported to offsite storage;

(v) paper documents containing personal data must be stored in locked/ secured location with limited access to authorised staff;

(vi) limited staff access rights to office areas storing confidential information;

(vii) provision of clear guidelines to staff as to the types of data that may or may not be disclosed to a phone enquirer and implementation of appropriate identity verification procedures to confirm the enquirer’s identity;

(viii) adoption of contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of personal data transferred to data processors (including cloud service providers);

(ix) adoption of data file integrity verification to ensure that the receiver gets the same file that the original sender intended. This is done by the original data sender providing a checksum or digital signature that confirms the integrity of a data file;

(x) adoption of password protecting and encrypting files to ensure that only the receiver with the password can access the file;

(xi) use of email data protection tool to ensure email senders double-check that they intended to send any email with potentially risky activities (e.g. containing sensitive data) to prevent any accidental unauthorised disclosure through email; and

(xii) use of data loss protection tools to prevent anomalous activities that are likely correlated with malicious activity or data incidents. Monitor computers, endpoint devices and files for anomalous activities (e.g. unexpected downloads of large amounts of sensitive data to personal computers) and stop any unauthorised file transfers.

**[*Note: For NGOs with more IT manpower and support, please consider adding the following security measures.*]**

(xiii) adoption of hashing with salt measure to ensure that sensitive values cannot be seen or reasonably recovered in the event of a compromise;

(xiv) adoption of tokenisation technique to ensure that identifiers cannot be seen in the event of a compromise. This measure replaces identifiers and attributes with a different value known only to the authorised users;

(xv) adoption of field-level encryption to ensure that sensitive values cannot be seen in the event of a compromise. It involves encrypting specific data fields to hide the true value. The underlying technique of field-level encryption achieves the same function as tokenisation, but is applied to different elements in the database (i.e., identifiers vs attributes). The technical implementation of field-level encryption uses a mathematical encryption function instead of a lookup table for tokenisation;

(xvi) adoption of obfuscation / masking / removal of entity attributes to ensure that the exact sensitive values cannot be seen or ever recovered in the event of a compromise, although approximate or noisy values might still be seen. This involves hiding the true value of the attributes by adding noise, banding the data, or masking out portions of the value. Attributes not relevant for data usage should be removed;

(xvii) adoption of dataset partitioning (of entities or attributes) to ensure that information on selected entities or attributes will not be compromised even if the larger database has been compromised. This could include protected personnel or sensitive attributes. This is done by breaking a dataset into smaller datasets by segmenting out select entities or attributes;

(xviii) use of digital watermarking of file to enable investigators to trace from whom the dataset originated from in the event of a data incident. This involves adding marking information such as a cryptographic signature. The watermark information can identify the originator of the dataset, prove the authenticity of the file, and is hard to remove from the file;

(xix) volume limited and time limited access to prevent officers from accessing too much data at one time, and the duration which the officer can access the data. Restrict data access when the duration and volume data access exceeds predefined limits; and

(xx) keeping logs and analysing them to flag anomalous activity as well as support remediation in the event of a data breach. Logging of data access to sensitive data at greater detail, such as to individual data query level. The logs should be protected from accidental or deliberate erasure, so that they can reliably show what data have been compromised, how they have been compromised and who was involved in the compromise.]

In addition, all electronic files containing personal data should be stored in the team’s shared drive as far as practicable. If creating or saving electronic files containing personal data in the local drive of a personal computer is required, such electronic files should be password protected.

**DPP5 - Transparency of the Personal Data Policy and Practices**

[\_\_\_\_] should take all reasonably practicable steps to make its personal data policies and practices known to the public.

[\_\_\_\_]’s Privacy Policy Statement (please refer to **Annex K** of this PMP Manual for a sample) is available for public access at its website or upon request sent to [*name*] at [*email address*].

All complaints and enquiries regarding personal data privacy policy and practices or [\_\_\_\_]’s compliance with the PDPO should be addressed to [*name*] by email at [*email address*] or by post to [*address*].

**DPP6 - Access to and Correction of Personal Data**

An individual has the right to (i) request access to his/her own personal data held by [\_\_\_\_] and (ii) request the correction of the personal data supplied if they are inaccurate. Please refer to **Annex B** of this PMP Manual for details of the Data Access and Correction Policy and the relevant steps to handle such requests from individuals.

All such requests should be handled by the Personal Data Privacy Officer. The identity of the requestor should be ascertained. If in doubt, [\_\_\_\_] may require the requestor to provide his/her identify proof.

A data subject may make a *data access request* to [\_\_\_\_] by completing the Data Access Request Form specified by the Privacy Commissioner. Please refer to **Annex C** of this PMP Manual for a copy of the form.

A data subject may make a *data correction request* to [\_\_\_\_] by completing the data correction request form specified by [\_\_\_\_]. Please refer to **Annex D** of this PMP Manual for a sample of the Personal Data Correction Request Form.

### **3.2.3 Direct Marketing**

**Direct Marketing – General[[24]](#footnote-24)**

[\_\_\_\_] must, before using personal data in direct marketing:

(i) inform the data subject of the intention to use the data in direct marketing;

(ii) obtain the data subject’s consent to the use of data in direct marketing and inform the data subject that it may not use the data unless it has obtained the data subject’s consent;

(iii) provide the data subject with information relating to the kinds of personal data to be used (e.g. name, e-mail address, phone number) and the classes of marketing subjects in relation to which the data are to be used;

(iv) provide the data subject with a channel through which the data subject may, without charge by the data user, communicate the data subject’s consent to the intended use (e.g. a telephone hotline, facsimile number, designated e-mail account, specific address to collect written responses or an online facility to allow data subjects to subscribe or unsubscribe or a designated person to handle requests from data subject); and

(v) notify the data subject that [\_\_\_\_] will, without charge to the data subject, cease to use the data in direct marketing if the data subject so requires.

[\_\_\_\_] must present the above information in a manner that is easily understandable and, if in written form, easily readable.

**Direct Marketing – Consent**

Consent is defined broadly to cover an indication of no objection to the use or provision of personal data for direct marketing purposes. To qualify as an indication of no objection, the data subject concerned must have explicitly indicated that he/she did not object to the use and/or provision of his/her personal data to another for use in direct marketing. Hence, consent cannot be inferred from the data subject’s non-response. In other words, silence does not constitute consent.

[\_\_\_\_] must not design any application or donation forms in such a way that renders it impracticable for data users to refuse the use of their personal data for direct marketing purposes. For example, it is common for a service application form to incorporate both the terms and conditions for provision of the data user’s services as well as statements relating to the use of the data collected for marketing products or services, or the provision of the personal data to a third party. If the customer is only provided with one space to sign on the form, he has to choose between (a) giving up the application for the service or (b) giving his “bundled consent” agreeing to the terms and conditions for the provision of the service as well as the use of his personal data as prescribed by the data user when in fact he finds such prescribed use objectionable. This is undesirable.

In such circumstances, [\_\_\_\_] shall design any application or donation forms in a manner that provides for the data subject’s agreement to the terms and conditions for the provision of the service to be separated from the data subject’s consent to the use of his personal data for direct marketing. Recommended ways to achieve this include providing a separate signature or tick box to indicate the data subject’s agreement or no objection to the prescribed use of his personal data.

**Direct Marketing – Cease to Use Personal Data in Direct Marketing**

A data subject may, at any time, require [\_\_\_\_] to cease to use the data subject’s personal data in direct marketing. [\_\_\_\_] must, without charge to the data subject, cease to use the personal data concerned upon receipt of such notification.

In order to comply with the data subject’s opt-out requirement effectively, [\_\_\_\_] has to maintain a list of all customers/applicants/members/non-members who have indicated that they do not wish to receive further marketing approaches (the “**Opt-Out List**”). [\_\_\_\_] has to adopt a systematic approach to comply with the data subjects’ requests for ceasing such use of their personal data. The Opt-Out List should be updated regularly.

Where the Opt-Out List is maintained via an online computer network, individual staff connected to the network have to input new opt-out requests as and when they are received. If the Opt-Out List is distributed other than by a computer network, it is recommended that staff members are notified of the updates at a frequency of no less than once per week.

[\_\_\_\_] must take all practicable steps to erase the personal data it held which are no longer required for the original purpose (including any directly related purpose) for which the data were collected. Hence, [\_\_\_\_] is required to make an assessment of the necessity of deleting all or some of the personal data of those customers/applicants/members/non-members who have indicated their opt-out requirements, and erase unnecessary personal data accordingly.

### **3.2.4 Risk Assessment Tools**

It is an important part of the PMP to ensure that the policies and practices of [\_\_\_\_] are and remain compliant with the PDPO. In view of this, both **periodic risk assessments** and **privacy impact assessments** should be performed to assess whether [\_\_\_\_]’s handling of personal data is aligned with the requirements under the PDPO, and whether there are potential material changes in the handling of personal data that could lead to potential data privacy risks.

**Periodic Risk Assessment**

Every year, [\_\_\_\_] should conduct periodic risk assessments to ensure that its privacy policies and practices comply with the PDPO. The [Personal Data Privacy Officer/Departmental Coordinators] should complete the risk assessment questionnaire and the Data Protection Officer should review the results. If any non-compliant issue is identified, the Data Protection Officer should draw up mitigation measures and rectify the non-compliant areas. Please refer to **Annex G** of this PMP Manual for a sample of the risk assessment questionnaire.

**[*Note: NGOs with more resources/manpower to designate Departmental Coordinators may consider setting forth the following Steps 1-5 governing the procedure for periodic risk assessment.*]**

**[Step 1 – Initiate the risk assessment and invite all / select the participating departments (Action by Data Protection Officer)**

The Data Protection Officer should initiate the assessment and invite all/select departments to participate in the periodic risk assessment. In selecting the departments to participate in the periodic risk assessment, the Data Protection Officer should consider the following:

• A department should participate in the periodic risk assessment at least once every 3 years;

• If a department holds a large amount of personal data, its risk assessment should be conducted at least annually; and

• If a department has changes/incidents that involve the handling of personal data, such as new initiatives launched, new data processors engaged, data breach incidents occurred or complaints received, etc., it should be selected in the year that the changes/incidents occur, or in the following year.

The Data Protection Officer should inform the Departmental Coordinators of every department of the commencement of assessment and provide the selected departments with the risk assessment questionnaires.

**Step 2 – Complete the Risk Assessment Questionnaire (Action by Departmental Coordinators)**

Departmental Coordinators of the selected departments should complete the risk assessment questionnaire and submit the completed questionnaire to the Data Protection Officer for review.

**Step 3 – Review the Risk Assessment Questionnaire (Action by Data Protection Officer)**

The Data Protection Officer should review the risk assessment questionnaires submitted by the Departmental Coordinators and identify whether there are any risks of non-compliance with the PDPO. If any risk areas are identified, he/she should inform and seek clarification from the respective Departmental Coordinators and proceed to Step 4. If no risk is identified, the Data Protection Officer should proceed to Step 5.

**Step 4 – Draw up mitigation measures (Action by Departmental Coordinators)**

After the Data Protection Officer has informed the Departmental Coordinators the risks identified, the concerned Departmental Coordinators should draw up mitigation measures in consultation with their respective Department Head, the Data Protection Officer and relevant subject officers. All risks identified should be addressed.

**Step 5 – File the Risk Assessment Questionnaire (Action by Data Protection Officer)**

If no risk is identified or all identified risks have been addressed, the Data Protection Officer should indicate so on the risk assessment questionnaire and file the questionnaire for record.]

**Privacy Impact Assessment (“PIA”)**

A PIA is a systematic process that evaluates the personal data privacy impact of the proposed changes in the handling of personal data, such as launching a new personal data handling procedure or launching a new project with the use of personal data, with the objectives of preventing and/or minimising adverse impacts. It provides [\_\_\_\_] an early warning by identifying and detecting any potential data privacy risks associated with the proposed changes before implementation.

A PIA should be undertaken –

(i) before the implementation of a new project or a change of policies and practices that involves:

• the processing or collecting of a considerable amount of personal data by [\_\_\_\_] or the data processors appointed; or

• collecting, processing, using or deleting personal data in ways that are materially different from [\_\_\_\_]’s existing practice; or

(ii) when there is a material change to the regulatory requirements relating to personal data and corresponding changes in the handling of personal data are required.

When the Data Protection Officer identifies the need to conduct a PIA, the PIA questionnaire should be completed and reviewed. The Data Protection Officer should ensure proper measures and controls are designed to address the identified privacy risks. If there is a change in the handling of personal data or a new project is launched, but the Data Protection Officer considers that there is no need to conduct a PIA (e.g. the change is of a relatively small scale), the Data Protection Officer should ensure that such consideration is properly documented. Please refer to **Annex H** of this PMP Manual for a sample of the PIA questionnaire.

### **3.2.5 Training and Education for Staff**

Continuous education and training are vital for maintaining staff awareness of the importance of data privacy. The following types of training and circulation of relevant information are recommended to be provided to [\_\_\_\_]’s staff:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Training activities** | **Target audience** | **Timing/Frequency** | **Actions to be taken by the Data Protection Officer** | **Target achievements** |
| Introduction of PMP | New comers | Once staff joins [\_\_\_\_] | - Provide new comers with this PMP Manual | Encourage new comers to read the materials in detail |
| Circulation of new/updated  data privacy policies and guidelines and highlights of updates in this PMP Manual | All staff | Whenever  there are any new or updated  data privacy  policies, guidelines or updated PMP Manual | - Send email notifications to staff  [- Upload the new policies and guidelines onto the intranet] | |  | | --- | | Provide staff with the new/updated policies and guidelines as soon as practicable | |
| Re-circulation of this PMP Manual and other data privacy policies and guidelines | All staff | Half-yearly | - By e-circulation  [- Upload the updated PMP Manual and other data privacy policies and guidelines to the intranet, if any] | Remind staff of the prevailing policies to ensure privacy awareness within [\_\_\_\_] |
| Training course/  Refresher course | All staff who handle a lot of personal data | When appropriate | - Notify staff members of the availability of the training | - Recap of the PDPO  - Data protection principles  - Operational needs on collection of personal data  - Security of personal data |

### **3.2.6 Data Breach Handling**

A data breach is a breach of security of personal data held by a data user, exposing the personal data to the risk of unauthorised or accidental access, processing, erasure, loss or use. Below are examples of data breaches:

• Loss of storage devices that contain personal data, e.g. notebook computers, USB flash drives, portable hard disks and paper files;

• Improper handling or accidental transmission of personal data, e.g. unauthorised disposal of files, sending personal data to a third party which is not supposed to receive the personal data;

• Information security incidents such as –

* Database containing personal data being hacked or accessed by outsiders/staff without authorisation;
* Leakage of personal data caused by the installation of file-sharing software in the computer, etc.; and

• Misact of the data processors, e.g. sharing of personal data by the service provider with unauthorised third parties.

**Data Breach Handling Guidelines**

When there is a data breach or when a data breach is suspected, the relevant officers should take prompt action to gather information and lessen the harm or damage that may be caused to the data subjects. [\_\_\_\_] should respond to a data breach as quickly as possible by taking the following actions:

- Report the breach to the Data Protection Officer and top management

- Gather essential information about the breach

- Consider notifying regulatory bodies

- Decide on the measures to contain the breach

- Assess the risk of harm

- Consider notifying the data subjects affected by the breach

- Investigate into the breach and report results

- Conduct post-incident review and consider improvement measures

A Data Breach Information Sheet should be completed for each data breach incident (please refer to **Annex I** of this PMP Manual). For further details of data breach handling, please refer to the “Guidance on Data Breach Handling and the Giving of Breach Notifications” issued by the Privacy Commissioner[[25]](#footnote-25).

**[*Note: NGOs with more resources/manpower may consider the following detailed steps for breach handling.*]**

**[Action – Report the breach to top management and other relevant staff members (Action by all relevant staff members)**

When there is a data breach or a possible breach, the subject officer should immediately report the matter to his/her Department Head. The Department Head should then report the breach to top management and notify the Data Protection Officer as soon as possible.

**Action – Gather essential information relating to the breach (Action by Department Head)**

The Department Head should, in consultation with the Data Protection Officer, gather the essential information about the breach and document the information in the “Information of the breach” section of the Data Breach Information Sheet (**Annex I** of this PMP Manual).

**Action – Consider notifying regulatory bodies (Action by Department Head)**

The Department Head should, in consultation with the Data Protection Officer, consider the circumstances of the breach and decide whether law enforcement agencies or any relevant regulators (e.g. the Hong Kong Police Force and the PCPD) should be notified. The Department Head should complete the “Data breach notification to regulatory bodies” section of the Data Breach Information Sheet, in consultation with the Data Protection Officer.

**Action – Decide on the measures to contain the breach (Action by Department Head)**

The Department Head should, in consultation with the Data Protection Officer, identify and adopt measures to contain the breach. The following containment measures should be considered:

***Measures applicable to the loss of portable storage devices storing personal data***

• Identifying the last-known location of the concerned storage device.

• Searching for the concerned storage device to retrieve the information therein as soon as possible, if practicable.

***Measures applicable to improper handling of personal data***

• Suspending the improper handling of personal data, such as stopping the inappropriate delivery or disposal of documents which contain personal data.

***Measures applicable to information security incidents***

• Suspending the system if the data breach is caused by a system failure.

• Changing the user passwords and system configurations to control access and use.

• Ceasing or changing the access rights of individuals suspected to have committed or contributed to the data breach.

• Engaging external technical assistance to remedy the system loopholes, if necessary.

• Keeping a backup image of the affected system for investigation purpose and as evidence for subsequent follow up action.

• Protecting sensitive or critical information and systems by means such as moving the critical information to other media (or other systems) which are separated from the affected system and its relevant network.

• Shutting down or isolating the compromised computer or system temporarily to prevent further damage to other interconnected systems.

After deciding on the breach containment measures, the Department Head should complete the “Actions taken/will be taken to contain the breach” section of the Data Breach Information Sheet, in consultation with the Data Protection Officer.

**Action – Assess the risk of harm (Action by Department Head)**

After deciding on the immediate actions to contain the breach, the Department Head should, in consultation with the Data Protection Officer, assess the risks associated with the breach to decide the next course of actions (e.g. should any public notification be made, should assistance be provided to affected data subjects, etc.).

The potential harm caused by a data breach may include:

• Loss of public trust

• Loss of assets (e.g. stolen computers or portable storage devices)

• Identity theft or fraud of the data subjects

• Reputational, psychological and/or material damage or loss of the data subjects

• Threat to personal safety of the data subjects

The extent of harm that may be suffered by the data subjects in a data breach depends on a number of factors, including the following:

• The type of personal data leaked – generally the more sensitive the data are (e.g. medical record or Hong Kong Identity Card number), the greater the damage it may cause to the data subjects;

• The amount of personal data involved – generally the greater the amount of personal data leaked, the more serious the consequences can be;

• The circumstances of the data breach – in case of online data leakage, it is usually difficult to prevent further dissemination and use of the leaked personal data.

• The likelihood of identity theft or fraud – sometimes the leaked data itself or when combined with other data could facilitate identity theft or fraud; and

• Whether the breach is an isolated incident or caused by a wider problem – if the breach is caused by a wider problem (e.g. the email server has been hacked), this may continue to jeopardise the security of personal data held by [\_\_\_\_] or cause further harm to the data subjects.

The Department Head should complete the “Risk of harm” section of the Data Breach Information Sheet, in consultation with the Data Protection Officer.

**Action – Consider notifying the data subjects affected by the breach (Action by Department Head)**

Having assessed the situation and the risk of harm of the data breach, the Department Head should, in consultation with the Data Protection Officer, consider issuing to the data subjects affected by the breach a **data breach notification**. Although it is not mandatory for [\_\_\_\_] as a data user to notify data subjects about the data breach, the consequences of failing to give notification (e.g. the impact on [\_\_\_\_]’s reputation and losing public trust) should be duly considered. If [\_\_\_\_] decides to issue a data breach notification, such notification should be issued as soon as practicable, except where law enforcement agencies have made a request for a delay for investigation purposes.

A data breach notification to data subjects should include the following information:

• A general description of what occurred;

• The date and time of the breach, and its duration (if applicable);

• The date and time the breach was discovered;

• The source of the breach (either by [\_\_\_\_] itself or the third party that processed the personal data);

• The types of personal data involved;

• An assessment of the risk of harm caused to the data subjects by the breach;

• A description of the measures already taken or to be taken to contain the breach;

• Information and advice on actions the data subjects can take to protect themselves from the adverse effects of the breach and against identity theft or fraud;

• The contact information of the Data Protection Officer for further information and assistance; and

• Whether the Hong Kong Police Force, the PCPD or other parties have been notified of the breach.

The notification to data subjects can be made by phone, in writing, via email or in person. When data subjects cannot be identified immediately or where public interest exists, public notification through media such as [\_\_\_\_]’s website or press release may be more effective.

The Department Head should document the analysis by completing the “Data breach notifications to data subjects affected” section of the Data Breach Information Sheet, in consultation with the Data Protection Officer.

**Action – Investigate into the data breach and report the investigation results (Action by Department Head and Data Protection Officer)**

After the data breach is under control, the Department Head should, in consultation with the Data Protection Officer, conduct an investigation into the breach to find out the root cause(s) of the breach and identify if the breach is related to an information system security problem, the personal data handling process or human error. When the investigation is completed, the Department Head/Data Protection Officer should report the investigation results to the top management as soon as practicable and document the investigation results by completing the “Investigation results” section of the Data Breach Information Sheet.

**Action – Conduct post incident review (Action by Data Protection Officer)**

The Data Protection Officer should review the Data Breach Information Sheet submitted by the Department Head, and should seek clarification for further information when necessary, to ensure information on the Information Sheet is accurately documented.

Based on the Data Breach Information Sheet and other relevant information, the Data Protection Officer should, in consultation with the Department Head involved in the breach, consider whether improvement measures (including administrative, procedural and/or technical measures, etc.) should be taken to reduce the likelihood of recurrence of similar breaches in the future. Possible improvement measures may include:

• Enhancement of security in handling personal data;

• Revision in the control of access rights of personal data granted to staff/data processors;

• Enhancement of IT security measures to protect personal data from hacking, unauthorised or accidental access, processing, erasure, loss or use;

• Revision of existing privacy policies and practices and/or the promulgation of new privacy policies and practices in light of the data breach with notification made to staff in writing;

• Strengthening of monitoring and supervision mechanism of staff and data processors;

• Additional provision of on-the-job training and circulation of information to promote privacy awareness and to enhance prudence, competence and integrity of the staff who are responsible for handling personal data; and

• Revision of appointment policy of data processors and review of the contractual terms with a data processor on protection of personal data privacy.

The Data Protection Officer should document the improvement measures by completing the “Post incident review” section of the Data Breach Information Sheet and submit it to top management for their information and record.]

### **3.2.7 Data Processor Management**

Data processor is defined as “a person who (i) processes personal data on behalf of another person; and (ii) does not process the data for any of the person’s own purposes”[[26]](#footnote-26). [Tasks performed by data processors engaged by [\_\_\_\_] include, but not limited to, the following –

• to carry out surveys;

• to input personal data into computer systems; or

• to scan documents which contain personal data.]

**Obligations of [\_\_\_\_] as a Data User Under the PDPO**

A data user is liable as the principal for the wrongful act of its authorised data processor.[[27]](#footnote-27) According to the PDPO, if [\_\_\_\_] engages a data processor, whether within or outside Hong Kong, to process personal data on behalf of [\_\_\_\_], [\_\_\_\_] **must adopt** contractual or other means to prevent (i) any personal data transferred to the data processor from being kept longer than is necessary for processing of the data[[28]](#footnote-28) and (ii) unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing[[29]](#footnote-29).

The types of obligations to be imposed on a data processor should include:

- Security measures to be taken by the data processor

- Timely return, destruction or deletion of the personal data no longer required

- Prohibition against other use and disclosure

- Prohibition against sub-contracting to other service providers

- Reporting of irregularity

- Measures to ensure contract staff’s compliance with the agreed obligations

- [\_\_\_\_]’s right to audit and inspect

- Consequences for breach of the contract

**Review of [\_\_\_\_]’s Management of Data Processors**

If [\_\_\_\_] engages a data processor, whether within or outside Hong Kong, to process personal data on its behalf, the Data Protection Officer and/or the Personal Data Privacy Officer should perform a review of the management of data processors **annually** by completing a Data Processor Review Checklist (please refer to **Annex J** of this PMP Manual for the checklist).

### **3.2.8 Communication**

[\_\_\_\_] should take all practicable steps to communicate its personal data policies and practices to the general public and staff.

**Communication to the Public**

In general, [\_\_\_\_]’s **Privacy Policy Statement** (“**PPS**”)is available for public access at [*website address*]or upon request sent to the Data Protection Officer. Please refer to **Annex K** of this PMP Manual for a sample of a PPS. For guidance on preparing a PPS, please refer to “Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement” issued by the PCPD.[[30]](#footnote-30) In particular, the PPS informs the public of –

(i) the purpose and manner of [\_\_\_\_] collecting personal data; and

(ii) their right to lodge a data access request or a data correction request, and the channel of lodging such requests, etc..

The Personal Data Privacy Officer of [\_\_\_\_] handles all complaints and enquiries relating to personal data protection in accordance with [\_\_\_\_]’s established complaints and enquiries handling procedures attached hereto as **Annex E**.

**Communication within [\_\_\_\_]**

The Data Protection Officer circulates this PMP Manual and other prevailing data privacy policies and guidelines to staff on **a half-yearly basis**, and keeps staff updated on any amendment to the PMP Manual and the relevant policies and guidelines.

### **3.2.9 Social Media Policy**

Social networks or social media are a common medium for NGOs for purposes of, among others, generating awareness and fundraising. [\_\_\_\_] may collect information from social networks. If it is practicable to ascertain, directly or indirectly, the identity of an individual from the information obtained by [\_\_\_\_] from the use of social networks, such information would most likely be regarded as “personal data” under the PDPO. In cases where the information collected from social networks does not contain unique identifiers of individuals, [\_\_\_\_] must carefully assess if such information, taken in its totality, can be used to directly or indirectly identify an individual. [\_\_\_\_] may collect a complex set of such information from social networks which, when combined together, and with or without other information [\_\_\_\_] may hold, may be sufficient to ascertain the identity of individuals. In such circumstances, the information collected may constitute personal data and the PDPO may apply.

**Social Network Marketing**

Social network marketing may be defined as a form of marketing activities conducted through the medium of social networks. It often involves producing contents that social network users are prompted to share with their friends or contacts. This sharing helps to increase brand/organisation exposure and “customer” groups reach.

Individuals should be notified and given the choice to opt-out if their social network behaviour and preferences (such as “liking” a particular brand/activity) are used for marketing purpose or being tracked. For example, if [\_\_\_\_] promotes to an individual’s contacts that the individual has shown interests in [\_\_\_\_], the individual should be made aware of this use of his/her information, and where technically feasible in the arrangement, allowed to opt out from participating in this marketing process.

[\_\_\_\_] may conduct certain marketing campaigns (e.g. membership programme and photo-sharing) through social networks which involve the explicit collection and use of personal data. The data of participants may be collected via a form or a web-based application developed for the social network specifically. Such collection of personal data is regulated under the PDPO. Among other requirements under the PDPO, [\_\_\_\_] must supply the corresponding PICS on or before collection of personal data and should also make clear in its PPS to data subjects its privacy policies and practices in relation to the personal data it handles. The PICS can be displayed as a “pop-up” screen online when a “confirm” button is pressed prior to the participants’ submission of personal data. Please refer to Annex A for a sample of a PICS and Annex K for a sample of a PPS.

**Photo-taking**

[\_\_\_\_] may take photos during its activities and publish them (with or without captions which may include personal data) on its social media for marketing or promotional purposes. A section on photo-taking should be included in the PICS and the PPS of [\_\_\_\_] to inform the data subjects. The data subjects should be informed that they can contact [\_\_\_\_] if they have any concerns or if they do not wish to have their images recorded for distribution.

If [\_\_\_\_] wants to publish a photo, to the extent personal data are involved, [\_\_\_\_] should check if those people in the photo have given consent, and if not, [\_\_\_\_] should get consent from such people before publishing the photo. However, not all photos are necessarily personal data. To constitute personal data, it must be practicable for the identity of the individual(s) to be directly or indirectly ascertained from the photos. As such, a photo merely showing a person’s visual image without mentioning his/her name or other personal data is normally not classified as personal data. Generally, [\_\_\_\_] may publish a group photo on social media if the identity of the individuals cannot be ascertained directly or indirectly from the photo. A photo just showing the individuals’ images without mentioning names or any other personal identifying information is normally not classified as personal data. As no personal data are involved, it is acceptable to post such a photo.

Please refer to “Privacy Implications for Organisational Use of Social Networks” issued by the PCPD[[31]](#footnote-31) for further information on what needs to be considered to safeguard personal data privacy when using social networks or social media to promote [\_\_\_\_].

### **3.2.10 Job Applicants Data Handling Policy**

[\_\_\_\_] obtains personal data of job applicants through its recruitment process.

**Advertising for Job Vacancies**

A PICS should be provided to the job applicants on or before collection of personal data. Recruitment advertisements that directly ask job applicants to provide their personal data (e.g. their personal resumes) should include a statement, as an integral part of the advertisement, informing applicants about the purposes for which their personal data are to be used, e.g. “*Personal data collected will be used for recruitment purposes only.*”; “*Personal data provided will be used strictly in accordance with [\_\_\_\_]’s personal data policies, a copy of which can be provided upon request*.” [\_\_\_\_] should not solicit personal data from job applicants in a recruitment advertisement that provides no identification of either [\_\_\_\_] or the employment agency acting on its behalf. If it is necessary to conceal [\_\_\_\_]’s identity in recruitment advertisements, [\_\_\_\_] may provide job applicants, upon request, with application forms that bear [\_\_\_\_] ‘s identity.

Where [\_\_\_\_] requires job applicants to fill in a job application form, either in a paper format or online on [\_\_\_\_]’s website, a practical way to comply with the PICS notification requirement is to print the PICS as an integral part of the application form or display it as part of the text of the online form. In the case of an online form, the PICS can also be displayed as a linked page to the online form or as a “pop-up” screen when a “confirm” button is pressed prior to the transmission of the online form.

**Personal Data Collected During Recruitment**

Personal data collected from job applicants should be adequate but not excessive. They should be relevant to the purpose of identifying suitable candidates for the job. Generally, these may include work experience, job skills, competencies, academic/professional qualifications, good character and other attributes required for the job. While it may be justifiable for [\_\_\_\_] to obtain the Hong Kong Identity Card number of a job applicant, say for checking it against those of previous unsuccessful applicants, [\_\_\_\_] should not collect a copy of the Hong Kong Identity Card during the recruitment process unless and until the individual has accepted an offer of employment.[[32]](#footnote-32)

If [\_\_\_\_] wishes to obtain references from a potential candidate’s current or former employers or other sources, [\_\_\_\_] should ensure that references are provided with the consent of the candidate concerned.

**Processing Applications for Employment**

[\_\_\_\_] should take all practicable steps to ensure that the personal data of job applicants are collected, processed and stored securely, irrespective of whether the data are stored in electronic, photographic or hard copy format. As a matter of good practice, databases comprising personal data of job applicants should be accessible only to authorised staff using secure passwords on a “need-to-know” basis. Hard copy data should be located in secure areas. In the event of such information being analysed or reviewed, the contents of that data should not be left unattended by, or out of the control of, authorised persons.

Personal data of unsuccessful applicants may be retained for a period of up to two years from the date of rejecting applicants and should then be destroyed. The data may be retained for a longer period if there is a subsisting reason that obligates [\_\_\_\_] to do so, or the applicants have given their consent for the data to be retained beyond two years. As a matter of good practice, an employer wishing to retain personal data relating to an unsuccessful job applicant, for the purpose of future recruitment exercises, should inform the candidate of the period for which the employer will normally retain such data. It is also a good practice to provide unsuccessful job applicants with the opportunity to request the destruction of their data if they do not wish them to be used for this purpose.

Please refer to “Code of Practice on Human Resource Management” issued by the PCPD[[33]](#footnote-33) for further information on handling of employment-related personal data.

## **3.3 Ongoing Assessment and Revision**

Assessment and revision of personal data policies and practices should be carried out annually to ensure effectiveness of the PMP. The assessment and revision involve two parts – (1) Prepare an oversight and review plan and (2) Review of the effectiveness of the PMP.

### **3.3.1 Development of an Oversight and Review Plan**

The Data Protection Officer should prepare an oversight and review plan, which must:

(i) cover the implementation of all programme controls;

(ii) cover all policies and procedures related to personal data privacy;

(iii) state when and how to conduct the assessment by whom, and set the assessment criteria;

(iv) include periodic assessment (at least once a year); and

(v) be endorsed by the [board of [\_\_\_\_]].

The following sample of an oversight and review plan is provided for reference.

|  |  |
| --- | --- |
| **Month** | **Oversight and review activities** |
| Jan – Apr | - Update personal data inventory  [- Review [\_\_\_\_]'s data processor management]  - Conduct periodic risk assessment  - Update training content and training plan |
| May - Jul | Assess the effectiveness of all PMP programme controls; and make corresponding amendments |
| Aug - Oct | Review and revise the PMP Manual as well as other personal data privacy policies and guidelines |
| Nov | Circulate the PMP Manual as well as other policies and guidelines related to personal data privacy to employees |
| Dec | Review the execution of the oversight and review plan; and prepare the plan for the next year |

### **3.3.2 Review of PMP’s Effectiveness**

In order to document the annual review on the effectiveness of the PMP, the Data Protection Officer and/or the Personal Data Privacy Officer should complete the following review table and confirm that the actions set out under the oversight and review plan have been carried out appropriately.

|  |  |  |  |
| --- | --- | --- | --- |
| **Action** | **Completed/Not completed** | **Date of last review/update** | **Difficulties observed and proposed mitigation measures** |
| 1. Update personal data inventory |  |  |  |
| 2. Periodic risk assessments |  |  |  |
| 3. Review and revise the PMP Manual and other personal data privacy policies and guidelines |  |  |  |
| |  | | --- | | 4. Update training content and training plan | |  |  |  |
| 5. Review of data breach handling mechanism |  |  |  |
| 6. Data processor review |  |  |  |
| 7. Updates on the PMP have been communicated to staff |  |  |  |

1. <https://www.pcpd.org.hk//english/resources_centre/publications/files/PMP_guide_e.pdf>. [↑](#footnote-ref-1)
2. Section 2(1) of the PDPO. [↑](#footnote-ref-2)
3. Data Protection Principle 2(4) in Schedule 1 to the PDPO. [↑](#footnote-ref-3)
4. Section 35A(1) of the PDPO. [↑](#footnote-ref-4)
5. <https://www.pcpd.org.hk/english/publications/files/GN_picspps_e.pdf> [↑](#footnote-ref-5)
6. Section 50A(1) of the PDPO. [↑](#footnote-ref-6)
7. Section 50A(2) of the PDPO. [↑](#footnote-ref-7)
8. Section 64(1) of the PDPO. [↑](#footnote-ref-8)
9. Section 64(3) of the PDPO. [↑](#footnote-ref-9)
10. Section 64(3A) of the PDPO. [↑](#footnote-ref-10)
11. Section 64(3B) of the PDPO. [↑](#footnote-ref-11)
12. Section 64(3C) of the PDPO. [↑](#footnote-ref-12)
13. Section 64(3D) of the PDPO. [↑](#footnote-ref-13)
14. Sections 19(1), 20 and 28(5) of the PDPO. [↑](#footnote-ref-14)
15. Sections 23(1) and 24 of the PDPO. [↑](#footnote-ref-15)
16. Section 64A of the PDPO. [↑](#footnote-ref-16)
17. Part 6A of the PDPO. [↑](#footnote-ref-17)
18. https://www.pcpd.org.hk/english/publications/files/GN\_DM\_e.pdf [↑](#footnote-ref-18)
19. Section 64A of the PDPO. [↑](#footnote-ref-19)
20. Section 50B of the PDPO. [↑](#footnote-ref-20)
21. Section 66E of the PDPO. [↑](#footnote-ref-21)
22. Section 66D of the PDPO. [↑](#footnote-ref-22)
23. https://www.pcpd.org.hk/english/doxxing/files/GN\_PDPAO\_e.pdf [↑](#footnote-ref-23)
24. This PMP Manual does not cover the use of personal data collected from third parties and the provision of personal data to another person for use by that other person in direct marketing. If [\_\_\_] proposes to do so, it is necessary to speak to its external legal adviser to find out the applicable legal and regulatory requirements. [↑](#footnote-ref-24)
25. https://www.pcpd.org.hk//english/resources\_centre/publications/files/DataBreachHandling2015\_e.pdf [↑](#footnote-ref-25)
26. DPP2(4) in Schedule 1 to the PDPO. [↑](#footnote-ref-26)
27. Section 65(2) of the PDPO. [↑](#footnote-ref-27)
28. DPP2(3) in Schedule 1 to the PDPO. [↑](#footnote-ref-28)
29. DPP4(2) in Schedule 1 to the PDPO. [↑](#footnote-ref-29)
30. See FN5. [↑](#footnote-ref-30)
31. https://www.pcpd.org.hk/english/publications/files/sn\_organisational\_e.pdf [↑](#footnote-ref-31)
32. Paragraph 3.3.2 of the Code of Practice on the Identity Card Number and other Personal Identifiers [↑](#footnote-ref-32)
33. https://www.pcpd.org.hk/english/data\_privacy\_law/code\_of\_practices/files/hrdesp\_e.pdf [↑](#footnote-ref-33)