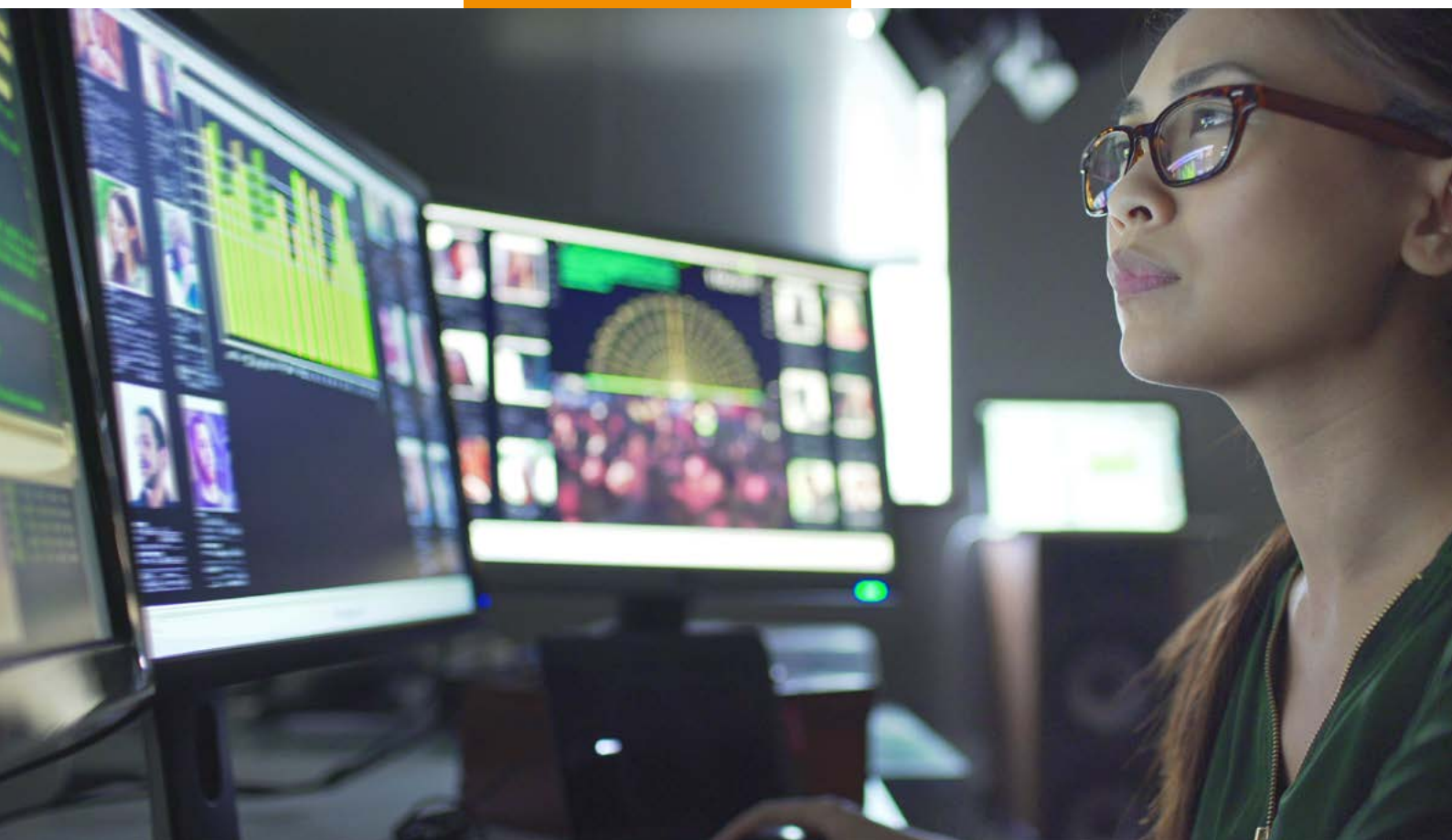


Personal Data Privacy Toolkit for NGOs





Building Trust through Strengthening Personal Data Protection and Compliance Capability of NGOs














Non-Governmental Organisations (NGOs) are at the forefront in identifying needs and gaps of services of the society, and providing social services to those in need. As a result, NGOs are the nexus of enormous amount of personal data ranging from user identification, and social support needs to surveillance, monitoring and evaluation. With the digitalisation of social services delivery and operations, data and information collected and stored by NGOs are increased at a progressive rate, and the broader use of digital platform could also impact NGOs' personal data compliance that they may not be familiar with.

As a user centric organisation, it is critical that NGOs comply with the Personal Data (Privacy) Ordinance (Cap. 486) to ensure data and information of their stakeholders (including users, funders, volunteers, service specialists, employees, etc.) are well protected, not only for compliance but more importantly, respecting the trust and confidence that their users and collaborators placed on them.

With a view to upskilling the operational capability of NGOs, this Personal Data Privacy Toolkit could facilitate them to comprehend the significance and implications of personal data protection and compliance in key areas of social services delivery as well as suggestions on how to develop compliance protocols and measures.

Index

Page

	Personal Data (Privacy) Ordinance	1
	DPP1: Purpose and Manner of Collection	5
	DPP2: Accuracy and Duration of Retention	6
	DPP3: Use of Data	7
	DPP4: Data Security	8
	DPP5: Openness and Transparency	10
	DPP6: Access and Correction	11
	Data Privacy Governance Structure	13
	Personal Data Inventory	14
	Privacy Impact Assessment	15
	Personal Information Collection Statement	16
	Data Breach Response	17
	Direct Marketing and Opt-Out Options	18

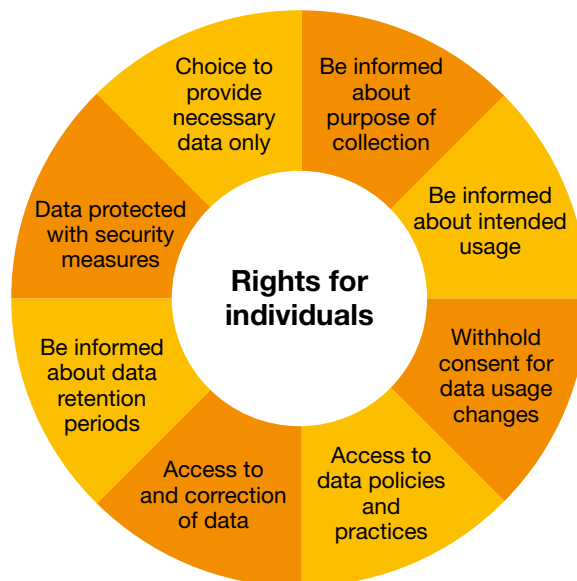


Personal Data (Privacy) Ordinance

Statutory Authority for Data Privacy and objective of the Ordinance

The office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD) is an independent statutory authority established to oversee the enforcement of the Personal Data (Privacy) Ordinance (Cap. 486) (Ordinance or PDPO). Its mission is to secure the protection of the privacy of individuals with respect to personal data through promotion, monitoring and supervision of compliance with the Ordinance.

The Ordinance aims to protect privacy rights related to personal data, i.e. recorded information relating directly or indirectly to a living individual (data subject), from which it is possible to ascertain the identity of the individual, and in a form where access to or processing of the data is practical. Any person who controls the collection, holding, processing or use of the personal data should comply with the requirements under the Ordinance.



Introduction of Six Data Protection Principles

A person who collects, holds, processes or uses personal data (i.e. data user) has to follow the six Data Protection Principles (DPPs) with the purpose of safeguarding the right of any individuals, known as data subjects. DPPs represent the core of the Ordinance and cover the entire life cycle of a piece of personal data including collection, retention, usage, sharing, transferring and destruction.

DPP1: Purpose and Manner of Collection

- Personal data must be collected in a lawful and fair way, for a purpose directly related to a function /activity of the data user.
- Data subjects must be notified of the purpose and the third parties to whom the data may be transferred.
- Data collected should be necessary but not excessive.

DPP2: Accuracy and Duration of Retention

- Personal data must be accurate and should not be kept for a period longer than is necessary to fulfil the purpose for which it is used.

DPP3: Use of Data

- Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless voluntary and explicit consent for the new purpose is obtained from the data subject.

DPP4: Data Security

- A data user must take practical steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

DPP5: Openness and Transparency

- A data user must make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

DPP6: Access & Correction

- A data subject must be given access to his/her personal data and allowed to make corrections if it is inaccurate.

Definition of Data Subject, Personal Data and Data User according to the Ordinance

Personal Data	<p>Personal Data means data:</p> <ol style="list-style-type: none"> 1. relating directly or indirectly to a living individual; 2. from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and 3. in a form in which access to or processing of the data is practicable. 	<p>Examples:</p> <ul style="list-style-type: none"> • personal particulars, e.g. name, personal identity ID, gender, date of birth, age etc. • contact details, e.g. mobile number, email address, correspondence address etc. • other information, e.g. marital status, credit card number, educational background, medical information, criminal conviction etc.
Data Subject	<p>Data subject is a living individual who is the subject of the personal data.</p>	<p>Examples:</p> <ul style="list-style-type: none"> • service users, volunteers, staff and donors/funders etc.
Data User	<p>Data user is a person who, either alone or jointly or in common with other persons, control the collection, holding, processing or use of data.</p>	<p>Examples:</p> <ul style="list-style-type: none"> • service providers • third parties engaged by service providers • collaborating service partners

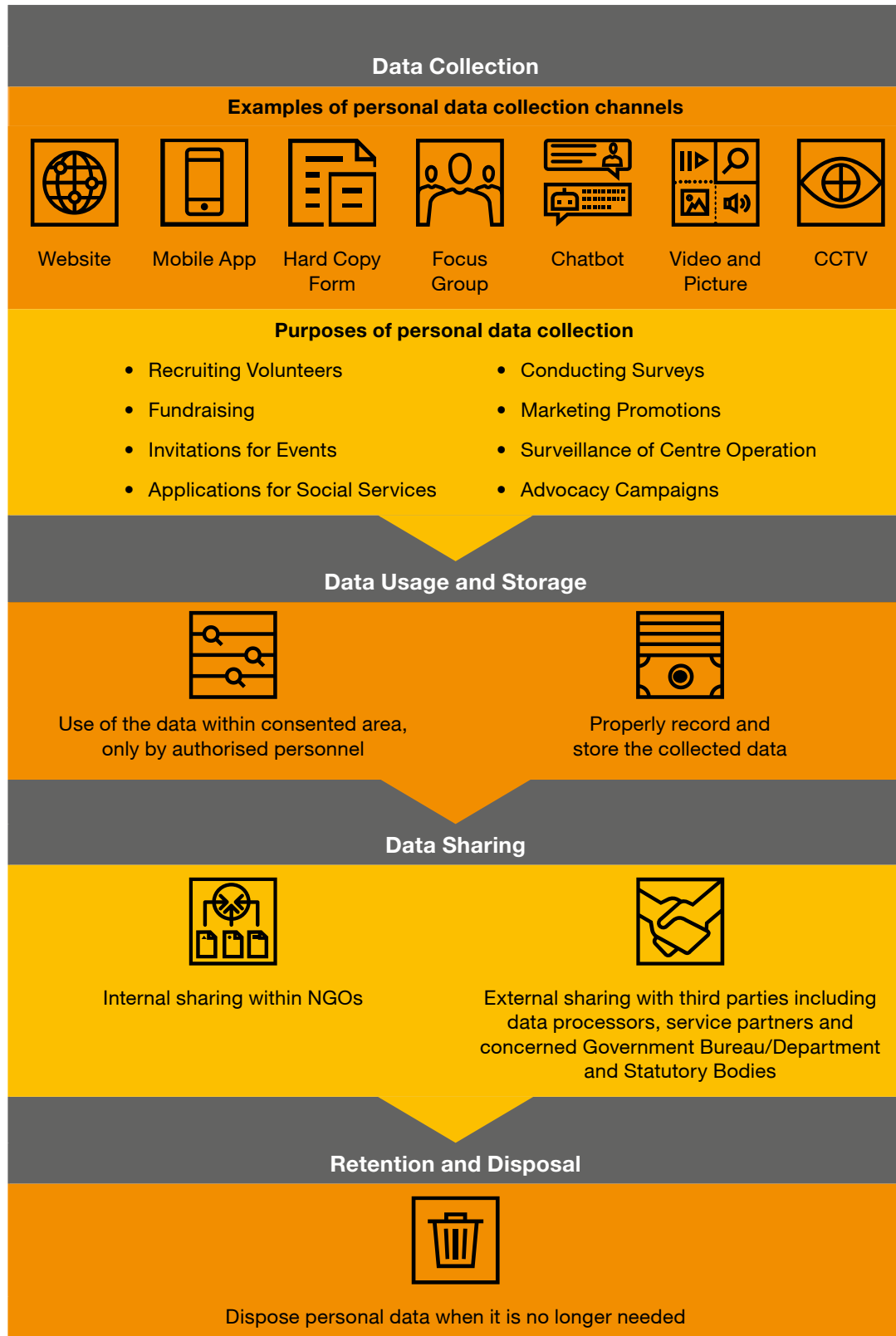
Offences and Compensation when not complying with the Ordinance

If any NGOs do not comply with the Ordinance, the Privacy Commissioner may serve an Enforcement Notice for the purpose of directing the NGOs to remedy the contravention and/or instigate the prosecution action. Contravention of an enforcement notice raised by the Privacy Commissioner is considered an offence which could result in a maximum fine of HK\$50,000 and imprisonment for 2 years, with a daily penalty of HK\$1,000. Subsequent convictions can result in a maximum fine of HK\$100,000 and imprisonment for 2 years, with a daily penalty of HK\$2,000.

Moreover, inappropriate use of personal data related to direct marketing activities is liable on conviction to the following:

Fine	Imprisonment	Description of Offence
HK\$500,000	3 years	<ul style="list-style-type: none"> • Failure to obtain prescribed consent (which is an express consent of the person given voluntarily) from data subjects regarding usage of personal data for direct marketing activities. • Failure to obtain prescribed consent from data subjects regarding disclosure of personal data to third parties for direct marketing activities with the purpose other than gain. • Failure to comply with request (opt-out option) from data subjects to cease to use their personal data for direct marketing activities.
HK\$1,000,000	5 years	<ul style="list-style-type: none"> • Failure to obtain prescribed consent from data subjects regarding disclosure of personal data to third parties for direct marketing activities with the purpose of gain.

Example of Personal Data Life Cycle



Examples of Data Privacy Risk that NGOs may face

- 01**
Inexperienced data handling practices and management.
- 02**
Access to personal data by unauthorised personnel.
- 03**
Personal data is kept longer than necessary.
- 04**
Excessive collection of personal data / data collected without prescribed consent.
- 05**
Inadequate security measures for data protection.
- 06**
Lack of data breach handling procedures.
- 07**
Lack of data privacy awareness.
- 08**
Insufficient monitoring of outsourcing activities to vendor / third parties.
- 09**
Personal data is not completely erased when it is no longer needed.



DPP1: Purpose and Manner of Collection

What is the Purpose and Manner of Collection Principle?

NGOs collect a lot of personal data in their daily operations. However, it is important to consider a few simple questions before you start collecting personal data, for example, what is the purpose and rationale to collect such personal data? Is it compulsory to collect these data? Are you collecting more than you need?

DPP1 of the Ordinance provides compliance requirements for NGOs which need to collect personal data from the service users, volunteers and donors or funders.



NGOs should consider the following when collecting personal data

01

Clearly think about and document how and why personal data needs to be collected and processed. Only collect data that is necessary for a specific purpose.

02

The means of personal data collection is lawful (e.g. data subjects are aware of collection of their personal data instead of through deception or coercion).

03

Understand operational processes which involve personal data.

04

Use a Personal Information Collection Statement (PICS) to communicate to data subjects why their personal data is being collected.

You may make reference to the Code of Practice on the Identity Card Number and other Personal Identifiers Compliance Guide for Data Users leaflet issued by the Privacy Commissioner:
https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/compliance_guide_e.pdf



DPP2: Accuracy and Duration of Retention

What is the Accuracy and Duration of Retention Principle?

DPP2 of the Ordinance requires that personal data collected and maintained by the NGOs to be accurate, complete, and up-to-date for the purpose for which it is to be used.

As personal data is collected from data subjects from various channels and programmes organised by NGOs at different times, the personal data maintained by NGOs can become outdated or inaccurate. There may also be limited governance over the retention and disposal of personal data which can result in data being kept for a period longer than necessary.

For example, personal data associated with an individual's account on NGOs' platform (e.g. website or mobile app) should only be retained for an appropriate period of time after de-registration. To meet this requirement, NGOs should establish a well-defined disposal mechanism to erase such personal data once the retention period is expired.

NGOs should consider the following when maintaining personal data

01 Accuracy

NGOs should ensure personal data they hold is accurate and provide a channel (e.g. via email) for data subjects including volunteers, service users, donors or funders to update their personal data.



02 Retention

Data retention periods are how long personal data should be kept by NGOs upon data collection and before disposal. NGOs should define data retention periods based on the original purpose for that data being fulfilled and ensure all personal data is disposed of when it is no longer necessary.



03 Disposal

Data disposal refers to erasing the personal data when it is no longer needed regardless of whether it is in digital or physical format. NGOs should establish detailed procedures governing how personal data should be erased according to its disposal schedule, and ensure such data is completely erased and can not be retrieved.





DPP3: Use of Data

What is the Use of Data Principle?

Personal data should only be used for the purpose for which data is collected for or for a directly related purpose. Exceptions to this are where there is voluntary and explicit consent for a new purpose obtained from the data subject. Often, NGOs may potentially use the personal data collected for other purposes like direct marketing of programmes and fundraising. Questions arise including: Should the NGOs inform the data subjects? What should NGOs do to stay compliant with the Ordinance requirements and be transparent when using personal data for additional purposes?

NGOs should consider the following when using personal data

01

Provide Personal Information Collection Statement (PICS) to data subjects whenever using personal data for new purposes.

02

Obtain prescribed consent for using personal data in direct marketing activities.

03

Provide data subjects with flexibility to change their preference on his/her consent at any time without charge.

04

Establish a mechanism to keep track of a data subject's consent and monitor consent usage.

If NGOs would like to use the collected personal data for direct marketing activities, a voluntary and an explicit consent has to be obtained from the individuals involved. A separate or revised PICS should be provided and communicated to the individuals concerned. You can refer to [page 16](#) of this Toolkit for the details of PICS.



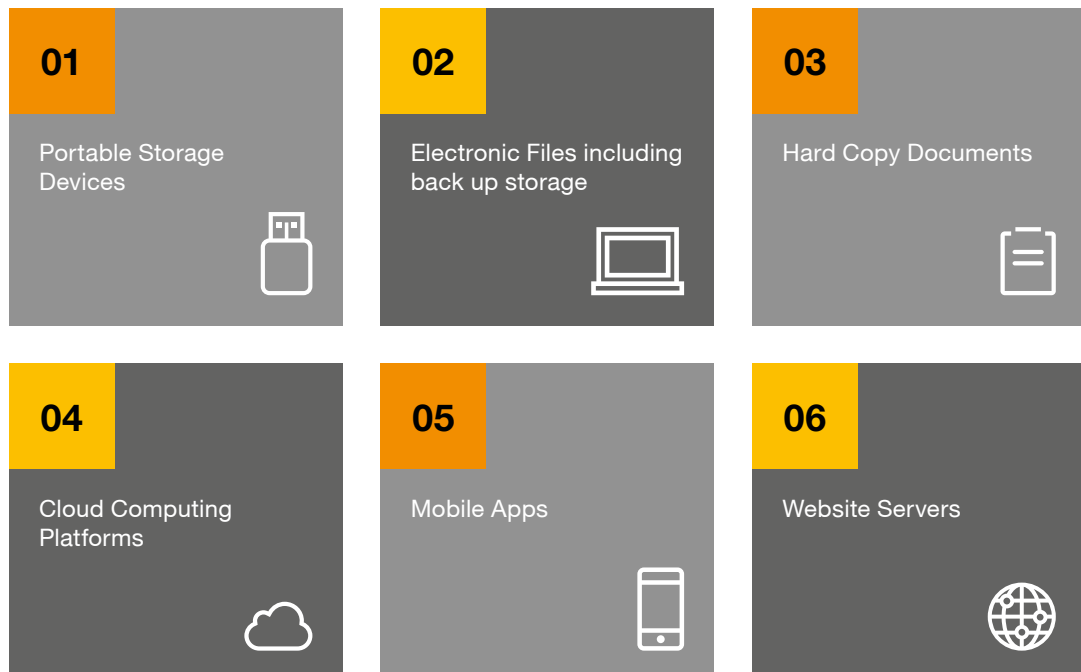
DPP4: Data Security



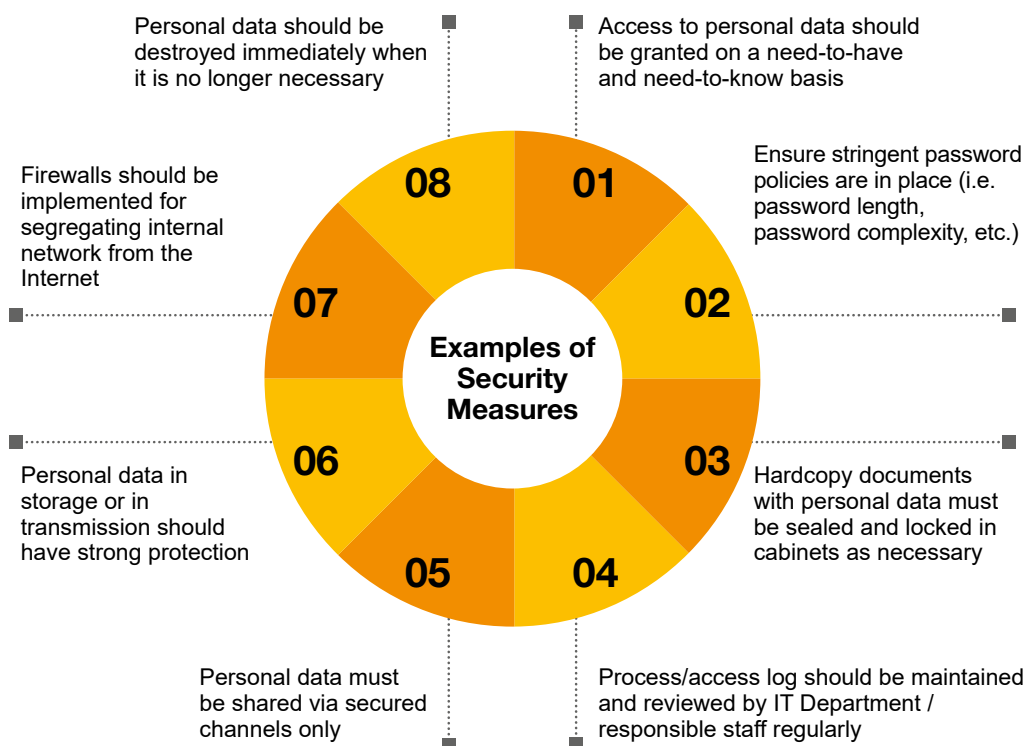
What is the Data Security Principle?

There has been a growing number of data breaches in recent years. One of the root causes of such incidents is due to inadequate controls over data security. DPP4 of the Ordinance requires NGOs to safeguard individuals' personal data and protect the personal data provided to third party data processors for processing.

Personal data could be stored in different media formats



What security measures should NGOs consider when storing, processing and transmitting personal data?



Online Behavioural Tracking

When NGOs deploy online tracking on their websites, for example by using cookies, that involve the collection of personal data of website users, NGOs should follow the six Data Protection Principles regarding the collection, holding and use of the personal data.

Data users should also ensure direct marketing activities are carefully managed and personal data is properly safeguarded if contractors (such as firms providing analytics on website visits) are engaged when carrying out online behavioural tracking.

Where cookies are used to collect behavioural information, NGOs are recommended the following:

1. To pre-set a reasonable expiry date for cookies.
2. To encrypt the contents of cookies whenever appropriate.
3. Not to deploy techniques (e.g. Flash, Zombie, Supercookies) that ignore browser settings on cookies unless NGOs can offer an option to website users to disable or reject such cookies.

You may make reference to the Online Behavioural Tracking information leaflet issued by the Privacy Commissioner.

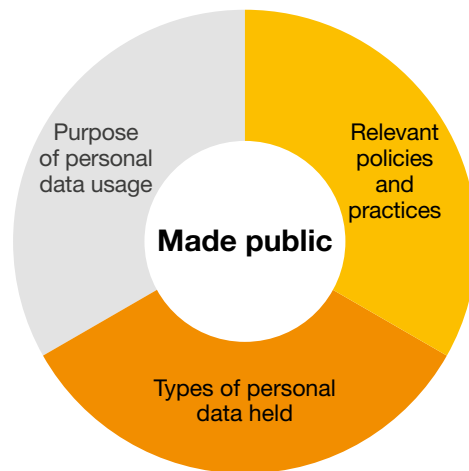
https://www.pcpd.org.hk/english/publications/files/online_tracking_e.pdf



What is the Openness and Transparency Principle?

In this Digital Age, it is important for NGOs to protect personal information and equally important for individuals to keep a watchful eye on data users that hold their personal data. DPP5 of the Ordinance requires NGOs to take all practical steps to make known to the public their policies and procedures in relations to handling personal data.

In order to effectively communicate its data handling practices with individuals; and, for the avoidance of doubt, NGOs are recommended to provide personal data policies and procedures in written format. It is a good practice for NGOs to establish a written statement, which is commonly known as a Privacy Policy Statement, to describe how personal data is handled.



What is a Privacy Policy Statement?

A Privacy Policy Statement (PPS) is a general statement about a data user's (e.g. NGO) privacy policies and practices in relation to the personal data it handles. A PPS should be made generally available to anyone, in an easily accessible manner, for example through website and pamphlets.

NGOs should also take the initiative to inform data subjects whenever there are any amendments to the PPS.

Key considerations of a Privacy Policy Statement

1. What is NGO's commitment to protecting personal data privacy?
2. What kind of personal data is held by the NGO and how it use the data?
3. Whether the NGO collect the personal data from minors or without individuals' knowledge e.g. through usage of cookies?
4. How long would the personal data be retained?
5. How does the NGO handle the personal data and whether it would be disclosed to third parties?
6. How does the NGO protect the personal data and whether any service providers would process personal data?
7. What are the security measures in place to protect the personal data collected?
8. Who and how to contact at the NGO for data access and data correction requests?

You may make reference to the Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement issued by the Privacy Commissioner:
https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_picspps_e.pdf



DPP6: Access and Correction

What is the Access and Correction Principle?

After collecting the personal data from data subjects, NGOs are responsible for ensuring that the personal information of the individuals is accurate. Therefore, NGOs are required to establish a mechanism for data subjects to access to his/her personal data, verify its accuracy and make correction if necessary. DPP6 of the Ordinance is in place to guide NGOs to handle the data subject access requests.

NGOs should explicitly inform the data subjects regarding his/her rights to request access to and correction of their personal data. It is a good practice to communicate such rights on or before the collection of personal data from individuals via Personal Information Collection Statement (PICS). NGOs, except if there are valid reason for refusing the request (e.g. failure of verifying requestor's identity), are required to comply with the request within 40 calendar days according to the Ordinance.

NGOs should consider the following when handling data subject access and/or correction requests

01

Define policies and procedures for handling data subject access and correction request to ensure that NGOs could respond to the request within the statutory time frame of related regulatory requirements.

02

Establish PICS and communicate to data subjects for their rights of access to and correction of personal data.

03

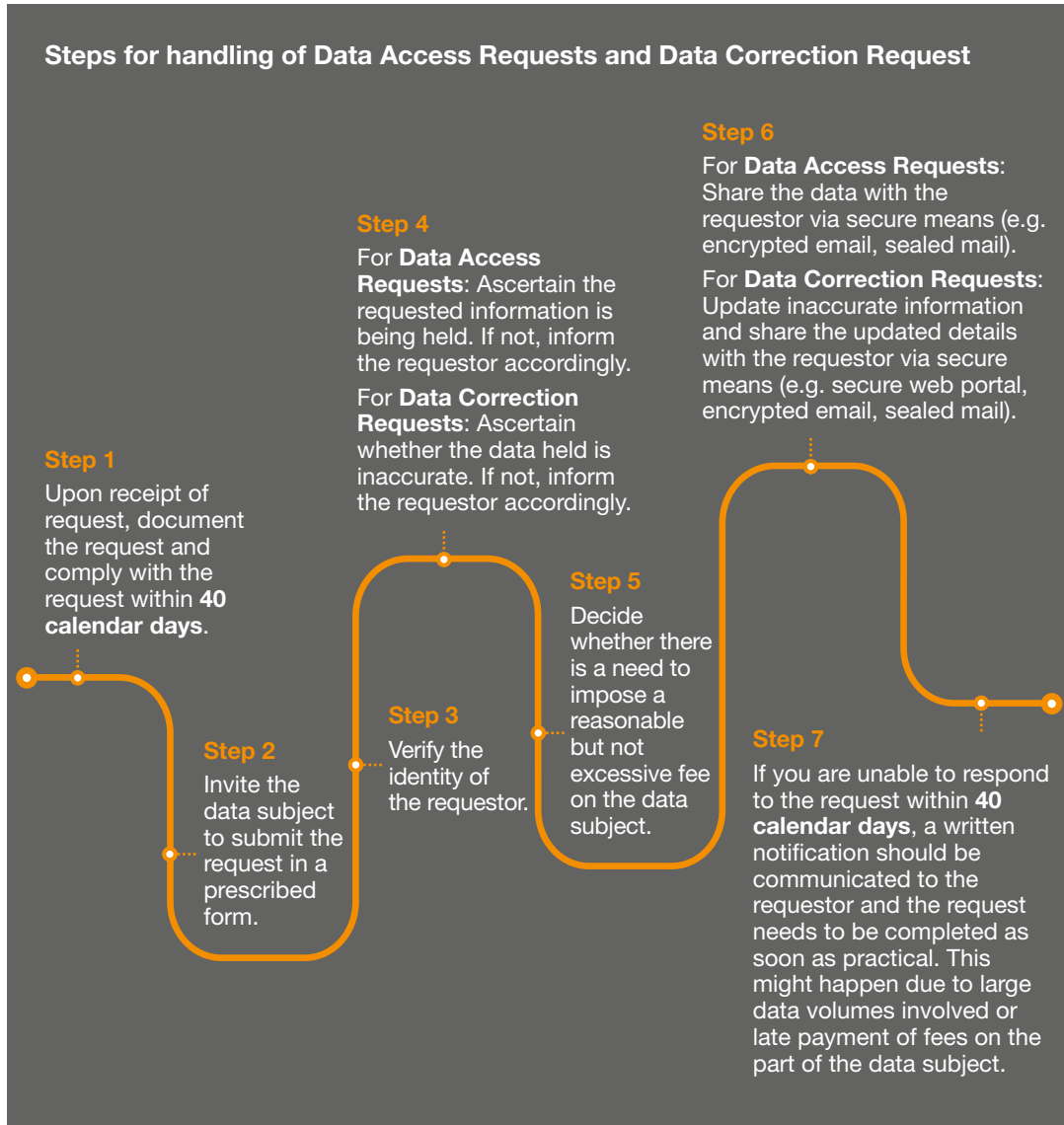
Designate a person responsible for handling all data access and correction requests. The contact details should be included in the PICS. All the requests should be formally documented.

04

Keep a log entry containing the reasons for refusal of data access and/or correction requests for four years.

Guidelines for Data Access and Correction Management

To comply with the DPP6, NGOs should establish detailed guidelines with steps for handling data subject access and/or correction requests raised by the data subjects. An example of how to handle these requests are set out below for reference:



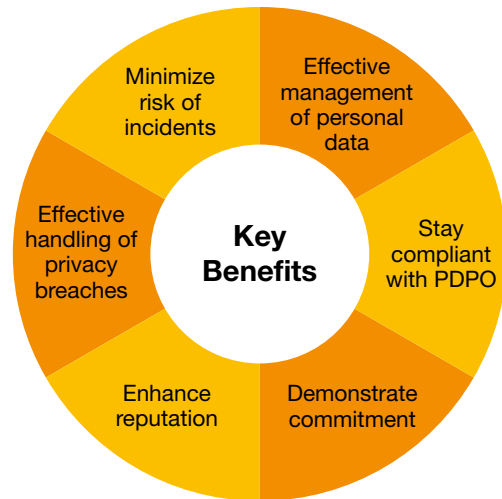


Data Privacy Governance Structure

Establishing a Data Privacy Governance Structure

With increasing public awareness and expectations for personal data privacy, NGOs have to implement stringent protection measures instead of merely treating personal data protection as a compliance issue. An internal governance structure is important to foster a data privacy culture and ensure that the policies and procedures on personal data protection are being followed. By defining data privacy roles and responsibilities, NGOs can embrace personal data protection as part of their daily operation responsibilities and implement relevant measures across their organisation. This can help in building trust with working partners and service users as well as strengthening community's confidence in engaging with NGOs.

Benefits of establishing a Data Privacy Governance Structure



Key roles and responsibilities in a typical Data Privacy Governance Structure

NGO leaders could lead by example and demonstrate their commitment to protecting personal data by cultivating a data privacy culture within their organisation. The following are some key roles and responsibilities in a Data Privacy Governance Structure for reference:



Board / Senior Management

Examples of roles and responsibilities of Board / Senior Management include:

- Developing and fostering a sound data privacy and protection culture.
- Formulating an overall data privacy vision and strategy.
- Overseeing key data privacy and protection risks.
- Providing oversight and assurance to the development of privacy policies and procedures.



Data Protection Office / Data Protection Officer

Depending on the size of the NGOs, it is recommended to appoint a designated personnel as the Data Protection Officer (DPO) or a team of staff should take up the role of DPO. Examples of roles and responsibilities of DPO include:

- Maintaining a complete and accurate record of the NGO's personal data inventory.
- Providing updates on privacy related policies in response to regulatory changes.
- Initiating periodic risk assessment over personal data to all departments.
- Handling data access and correction request made to the NGO, and privacy related complaints and enquiries.
- Conducting training and distributing educational materials to promote staff awareness on privacy protection.

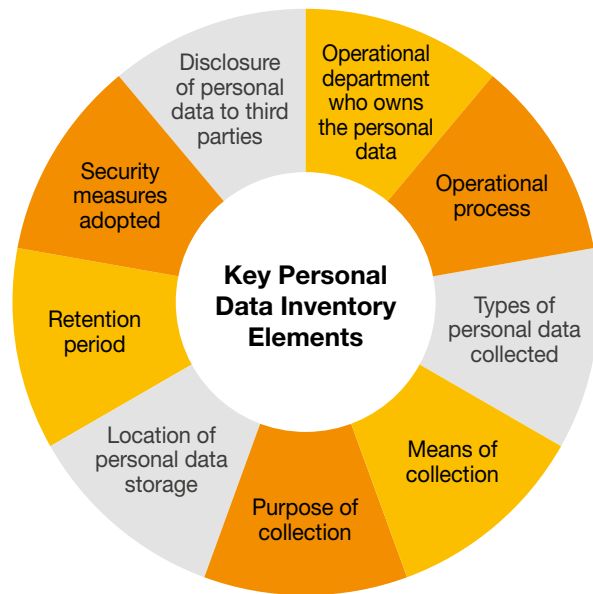


What is a Personal Data Inventory?

A Personal Data Inventory refers to a record of personal data assets. It consists of details including, but not limited to, types of personal data collected, the means of collecting personal data, locations for data storage, duration of retention, ways of using personal data and data security measures adopted.

The overarching objective for an NGO to create a personal data inventory is to understand the types of personal data collected and how the personal data is being processed.

Reviewing and updating the personal data inventory periodically (at least annually) could provide NGOs an up-to-date and accurate view of the personal data held by the organisation.



Advantages of maintaining a Personal Data Inventory

- Support data subjects to access and/or correction process as the data inventory provides exact location and data elements being collected.
- Understand the type and volume of personal data the NGO is collecting from data subjects.
- Determine the level of security measures to be in place (e.g. stringency of security controls should commensurate with the level of sensitivity of personal data).
- In the event where data breach occurs, it allows timely assessment by locating the types of personal data and the volume of personal data impacted.

PCPD has prepared a template for the preparation of Personal Data Inventory, you may refer to p.44 of the Privacy Management Programme for a sample:

https://www.pcpd.org.hk/pmp/files/pmp_guide2018.pdf



Privacy Impact Assessment

What is a Privacy Impact Assessment?

A Privacy Impact Assessment (PIA) is a systematic risk assessment tool that can be integrated into the decision-making process when launching projects or programs that required collection of personal data.

Examples of when a PIA is triggered

- New or modification to the current processes which is likely to result in a high degree of risk for individuals.
- Marketing initiatives include collection of significant amount/sensitive personal data.
- New initiatives or projects that collect/use large volume of personal data.
- Material change to regulatory requirements relating to personal data.
- Intention to engage data processors to handle personal data.
- Changes in the IT system infrastructure.

Why PIA is necessary?

A PIA offers NGOs an “early warning” by identifying and detecting any privacy related problems associated with a project before it is implemented. It should be undertaken by NGOs with a view to effectively managing privacy risks arising from a project that may involve:

- processing or storage or analysis of personal data, whether by the NGO or by an agent appointed by the NGO;
- implementation of privacy-intrusive technologies (e.g. installation of CCTV at workplace) that might affect a large number of individuals;
- major change in the NGO’s practices that may result in expanding the amount and scope of personal data to be collected, processed or shared.

Purpose of PIA

- Address privacy problems.
- Enable decision making.
- Provide a credible source of information.
- A cost effective way of reducing privacy risks.
- Provide benchmarks.



PCPD has prepared a template for performing a Privacy Impact Assessment, you may refer to p.49 of Privacy Management Programme for a sample:
https://www.pcpd.org.hk/pmp/files/pmp_guide2018.pdf



Personal Information Collection Statement

What is a Personal Information Collection Statement?

A Personal Information Collection Statement (PICS) is a statement provided by a data user (e.g. NGOs) to a data subject on or before collection of personal data. PICS is an important tool used for the purpose of complying with the notification requirements under the Purpose and Manner of Collection Principle of the Ordinance. To avoid misunderstanding between NGOs and data subjects, it is a good practice for NGOs to be transparent by presenting the required information of a PICS in a written format.

Key elements included in the PICS

01	Purpose: The purposes for which personal data collected will be used. For example, recruiting volunteers, fundraising, etc.	02	Whether it is obligatory or voluntary to provide individuals' personal data: If it is obligatory for data subjects to provide their personal data, the NGO should inform them of the consequences of failing to do so.	03	Potential transferees: Potential parties that the NGO may transfer and share the personal data obtained from data subjects. For example, Social Welfare Department and collaborating service partners, etc.
04	Direct marketing: If an NGO uses individuals' personal data for direct marketing, consent must be obtained from data subjects in advance. For example, individuals can choose to check the box in PICS to indicate whether their personal data can be used for direct marketing.	05	Rights of access to and correction of personal data: Inform data subjects of their rights of access to and correction of their personal data.	06	Contact details requesting access or correction: The name (and/or job title) and contact details of the individual who is responsible for handling any data access and data correction requests.

Good practices when writing a PICS



Purpose should be stated clearly

The purpose is recommended to enable data subjects to ascertain objectives of collection and usage of their personal data.



Language and presentation should be user-friendly

PICS is recommended to be presented in a manner which is easily readable and understandable in terms of its length, complexity, font size and accessibility.



Statement of security measures

A PICS is recommended to include a notice about the security measures adopted by the NGO to protect personal data.



Link to Privacy Policy Statement

A web link can be provided to draw the attention of data subject to the contents of the NGO's Privacy Policy Statement.

You may make reference to the Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement issued by the Privacy Commissioner:

https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_picspps_e.pdf



Data Breach Response

What is a Data Breach?



Personal data breach means a suspected breach of data security of personal data held by NGOs, exposing the data to risk of unauthorised or accidental access, processing, erasure, loss or use. Examples of data breaches include:

01	Loss of hard copy documents with personal data.	02	Accidental transmission of personal data via emails.	03	Unauthorized access to system with personal data.
-----------	---	-----------	--	-----------	---

Personal data breaches are expensive on many fronts. NGOs should consider developing procedures in relation to handling breach incidents and designating Data Breach Response Team with relevant roles and responsibilities, wherever feasible. This team could be led by a Data Protection Officer (if one has been appointed within the organisation) together with representative(s) of concerned department / team. When considering the team composition, you may consider including representatives from various functions, such as data protection office, communication and public affairs department, information technology department, legal and secretarial department, and human resources department, etc.

Containment measures for a Data Breach

Once a Data Breach is identified, NGOs should decide on the measures to contain the breach immediately in order to minimize the impacts and remediate the breach as soon as possible. The followings are some containment measures that NGOs could consider:

- | | |
|--|---|
|  terminating the system if data breach is caused by system failure |  retaining evidence of the data breach to facilitate investigation. If necessary, creating a backup image for investigation purpose |
|  changing the user's password and system configurations to control access and usage |  notifying relevant authorities i.e. PCPD and / or reporting to Police if criminal activities are suspected to have been conducted |
|  ascertaining if technical assistance is needed to repair system loopholes and/or stop the hacking |  protecting sensitive and critical information in systems with thorough overhaul of current operating environment, such as moving the information to other media |
|  ceasing or changing access rights of individuals suspected to have committed or contributed to the data breach |  directing data processor to take immediate remedial measures |

You may make reference to the Guidance on Data Breach Handling and the Giving of Breach Notifications issued by the Privacy Commissioner:

https://www.pcpd.org.hk/english/resources_centre/publications/files/DataBreachHandling2015_e.pdf



Direct Marketing and Opt-out Options

Direct Marketing

Direct Marketing are activities regarding (1) the offering, or advertising of the availability, of goods, facilities or services or (2) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes.

Direct marketing can include sending information or goods (addressed to specific persons by name) by mail, fax, electronic mail, telephone calls or other means of communication to specific people.

According to Use of Data Principle, if NGOs intend to use personal data for purposes of direct marketing activities, they have to clearly state this in the Personal Information Collection Statement (PICS) and seek prescribed consent from data subjects when such data was first collected for other stated purposes.



Direct marketing activities or not?

Examples of direct marketing

- A marketing SMS sending to the mobile phone number of a named individual.
- An NGO approaching its existing service users by telephone or emails to promote other upcoming events/ activities.

Examples of activities not considered direct marketing

- A marketing call to the unidentified owner of a particular telephone number for service provided by an NGO.
- Direct mail sent to an address without addressing a specific person by name.
- Notification of activity details without offering other services.

Opt-out Option

An Opt-out option is where a data subject may at any time require NGOs to cease using his/her personal data in direct marketing, irrespective of whether an earlier consent has been given by the data subject.

NGOs must cease using the personal data upon receipt of such notification from data subjects without imposing any charge. After receiving the opt-out request, NGOs may need to make an assessment of the necessity of deleting personal data of those individuals who have indicated their opt-out preference and then erase any unnecessary personal data accordingly.

Example of Opt-out Statement in a Personal Information Collection Statement

You may withdraw your consent for the use of your personal data for direct marketing purposes at any time by exercising your Opt-out right. Thereafter we shall cease using such data for direct marketing purposes.

If you wish to withdraw your consent, please contact our Data Protection Officer (name, contact details).

You may make reference to the Guidance on Direct Marketing issued by the Privacy Commissioner: https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_DM_e.pdf

If you have any questions about this toolkit, please contact:

Jennifer Ho

Risk Assurance Leader

PwC Mainland China and Hong Kong

jennifer.cw.ho@hk.pwc.com

Kristine Chung

Partner

PwC Hong Kong

kristine.ky.chung@hk.pwc.com

Shirley Gu

Senior Manager

PwC Hong Kong

shirley.y.gu@hk.pwc.com

The information contained in this toolkit is of a general nature only. It is not meant to be comprehensive and does not constitute the rendering of legal, tax or other professional advice or service by PricewaterhouseCoopers Limited (PwC). PwC has no obligation to update the information as law and practices change. The application and impact of laws can vary widely based on the specific facts involved. Before taking any action, please ensure that you obtain advice specific to your circumstances from your usual PwC client service team or your other advisers.

The materials contained in this toolkit were assembled in May 2020 and are based on information available at that time.

© 2020 PricewaterhouseCoopers Limited. All rights reserved. PwC refers to the Hong Kong member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details. PMS-000661