香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Privacy Management Programme

A Best Practice Guide

Contents

Privacy Management Programme
A Best Practice Guide

Introduction

Privacy Management Programme per se is not a requirement under the Personal Data (Privacy) Ordinance ("**the Ordinance**"). However, the Privacy Commissioner for Personal Data ("**the Commissioner**") advocates that organisational data users should embrace personal data privacy protection as part of their corporate governance responsibilities and apply them as a business imperative throughout the organisation, covering business practices, operational processes, product and service design, physical architectures and networked infrastructure. To this end, a **privacy management programme** serves as a strategic framework to assist an organisation in building a robust privacy infrastructure supported by an effective on-going review and monitoring process to facilitate compliance with the requirements under the Ordinance. It also demonstrates the organisation's commitment to good corporate governance and building trust with its employees and customers through open and transparent information policies and practices.

Constructing a **privacy management programme** within an organisation takes careful planning and consideration across disciplines and job functions. Employees should be aware of and understand the applicable parts of the organisation's **privacy management programme**. Customers and business partners should likewise be made aware of and given assurance, where appropriate, in the relevant aspects of the **privacy management programme**. Privacy-related obligations and risks should be correctly identified and appropriately taken into account in developing business models and related technologies and business practices before new products or services are launched. Risks of data breaches should be minimised and the effects of any data breaches mitigated.

There will be times when mistakes are made. However, with a solid **privacy management programme**, organisations will be able to identify their weaknesses, strengthen their good practices, demonstrate due diligence, and potentially raise the protection of personal data that they hold to a higher level than the bare minimum needed to meet legal requirements.

This Best Practice Guide ("**this Guide**") outlines what the Commissioner advocates as good approaches for developing a sound **privacy management programme**, but it is not a "one-size-fits-all" solution. Each organisation will need to determine, taking into consideration its size and nature of business, how best to apply this Guide to develop its own **privacy management programme**.

For the avoidance of doubt, this Guide does not constitute a Code of Practice under section 12 of the Ordinance or a Guidance Note which, in the traditional regulatory sense, provides direct guidance for compliance with specific provisions of the Ordinance. No specific legal liability will be incurred directly if an organisation elects not to observe the advice and recommendations contained in this Guide. The word "should" used in the context of this Guide represents the Commissioner's advocacy of the best practice instead of imposing prescriptive obligations to be met by organisations.

Part A of this Guide outlines the baseline fundamentals or components of a **privacy management programme**. Elements such as organisational commitment and programme controls are important.

Part B discusses how to maintain and improve a **privacy management programme** on an ongoing basis. A **privacy management programme** should never be considered a finished product; it requires ongoing assessment and revision in order to be effective and relevant. The components should be regularly monitored, assessed and updated accordingly to keep pace with changes both within and outside the organisation. This may encompass changes in such areas as technology, business models, law and best practices.

The Benefits of Implementing a Privacy Management Programme

Every organisation that is subject to the Ordinance is obliged to comply with the statutory requirements therein. A comprehensive **privacy management programme** provides an effective way for organisations to assure themselves of compliance. But it is more than that. It helps foster a privacy respectful culture throughout an organisation. This is conducive to building trustful relationships with customers, employees, shareholders and regulators.

When an organisation "walks the talk" by implementing a robust **privacy management programme**, enhanced trust from stakeholders including customers to engage with that organisation should follow. An organisation that has a strong **privacy management programme** may enjoy an enhanced reputation that gives it a competitive edge.

Conversely, without strong personal data protection, trust may erode to an organisation's detriment. Personal data breaches can be expensive for organisations – both in terms of "clean up" and reputation repair. Breaches may also prove expensive for the affected individuals.

Given the vast amounts of personal data held by organisations and institutions, the increasing economic value of the data, and the heightened attention and concern regarding privacy breaches, it makes business sense for organisations to take steps to put in place and maintain **privacy management programmes** to minimise the risks of such breaches, maximise the organisation's ability to address the underlying problems, and minimise the damage arising from breaches.

Developing a Comprehensive Privacy Management Programme

Part A – Baseline Fundamentals of a Privacy Management Programme

What should an organisation do to ensure that it is handling personal data appropriately? How will it know that it is doing it right? How will it be able to demonstrate to itself, its customers, the public and the Commissioner that it has the capacity to comply and has complied with the Ordinance?

Organisations are advised to appoint someone to oversee the development, implementation and maintenance of the organisation's personal data protection programmes and practices. Policies and processes are needed, and training of employees is required. Contracts (or other means) are required when organisations transfer personal data to data processors for processing, to ensure that the data is protected in a manner that is comparable to how the organisation would protect it. Organisations should have systems in place to respond to data access and correction requests from individuals for their personal data, and to respond to complaints from employees and customers about infringement of personal data privacy.

This part outlines the key components of a **privacy management programme**.

1 Organisational Commitment

This first component is an internal governance structure that fosters a privacy respectful culture.

Organisations should develop and implement programme controls that give effect to the data protection principles in Schedule 1 to the Ordinance. Compliance with the legal requirements in an effective and responsible manner, however, requires organisations to have a governance structure, or at the minimum, processes to follow and the means to ensure that they are being followed. A privacy respectful culture needs to be cultivated.

(a) Buy-in from the Top

*Top management support is key to a successful **privacy management programme** and essential for a privacy respectful culture.*

When top management is committed to ensuring that the organisation is accountable, the programme will have a better chance of success, and a privacy respectful culture will more likely be established.

Top management needs to support the **privacy management programme**. Depending on the organisation structure, top management or its delegated authority should:

- appoint the Data Protection Officer(s);
- endorse the programme controls; and
- report to the Board, as appropriate, on the programme.

(b) Data Protection Officer/Data Protection Office

Organisations should appoint or designate someone to manage the privacy management programme.

Whether this person is a senior executive of a major corporation or the owner/operator of a very small organisation, someone should be assigned responsibility for overseeing the organisation's compliance with the Ordinance (herein referred to as the "**Data Protection Officer**"). The Data Protection Officer may or may not be a full-time job. In larger organisations, the Data Protection Officer may need to be supported by dedicated staff. Also, while other individuals may be involved in handling personal data, the Data Protection Officer is usually the one responsible for structuring, designing and managing the programme, including all procedures, training, monitoring/auditing, documenting, evaluating, and follow-up. Resources should be channeled to train and develop the Data Protection Officer and/or his team as a professional in personal data privacy protection.

The Data Protection Officer can play many roles with respect to personal data protection. Typically, the Data Protection Officer will:

- establish and implement programme controls;
- coordinate with other appropriate persons responsible for related disciplines and functions within the organisation;
- be responsible for the ongoing assessment and revision of programme controls;
- represent the organisation in the event of an enquiry, an inspection or an investigation by the Commissioner; and
- advocate personal data protection within the organisation itself.

The last role is as important as the others. Organisations face competing interests and personal data protection is one programme of many. Personal data protection should be seen not just as legal compliance but also in terms of improving processes, customer relationship management, and reputation. The **privacy management programme**'s importance should be recognised at all levels. It is important to build this into every major function involving the use of personal data, including product development, customer services or marketing initiatives.

(c) Reporting

Reporting mechanisms should be established, and reflected in the organisation's programme controls.

The organisation should establish internal reporting mechanisms to ensure that the right people know how the **privacy management programme** is structured and whether it is functioning as expected. Within larger organisations, the audience for this information is likely to be top management, and in turn, top management reports to the board of directors. All reporting mechanisms should be reflected in the organisation's programme controls.

Organisations should establish some form of internal audit and assurance programmes to monitor compliance with their personal data protection policies. This could include the form of customer and employee feedback for smaller organisations, or for some larger organisations, third-party verifications. Should the organisation be subject to an enquiry, an inspection or an investigation under the Ordinance, these reports may be helpful in demonstrating the organisation's compliance with the Ordinance.

However, there is more to reporting than this. There will be times when escalation of personal data issues should be considered, for example, when there is a security breach or in case of complaints. Escalation means both involving people of relevant responsibility and ensuring that the needed persons in the organisation are included in the resolution of the issue. In large organisations, this could include, for example, representatives from technical, legal and corporate communications streams. How and when to escalate should be clearly defined and explained to employees. To ensure that related processes are being followed, organisations may need to monitor whether the necessary steps are being taken when triggered. Some organisations have found it useful to conduct test runs, for example, for their personal data breach identification, escalation and containment protocols.

An effective reporting programme:

- clearly defines its reporting structure (in terms of reporting on its overall compliance activities) as well as employee reporting structures in the event of a complaint or a potential breach;
- tests and reports on the results of its internal reporting structures; and
- documents all of its reporting structures.

2 Programme Controls

Programme controls form the second component of a **privacy management programme**. These help ensure that what is mandated in the governance structure is implemented in the organisation. This section identifies the programme controls in a **privacy management programme**. Developing these controls will assist the Data Protection Officer in structuring

an appropriate **privacy management programme** within the organisation and the controls will be used to demonstrate how the organisation is compliant with the Ordinance.

(a) Personal Data Inventory

*Whether it has a sophisticated **privacy management programme** in place or is implementing a new one, every organisation can benefit from carefully examining the personal data it holds and how it currently handles the data.*

An organisation should know what kinds of personal data it holds (for example, personal data of employees, personal data of customers, etc.), how the personal data is being used – and whether the organisation really needs it at all. Understanding and documenting the types of personal data that an organisation collects and where it is held (e.g. whether or not the data has been passed to any data processor) are important. This will affect the type of consent the organisation obtains from individuals and how the data is protected; and it will make it easier to assist individuals in exercising their data access and correction rights. Every component of an accountable, effective **privacy management programme** begins with this assessment.

Every organisation should be clear about:

- what kinds of personal data it holds and where it is held (i.e. within the organisation or by the data processor(s)) and document this assessment; and
- why it is collecting, using or disclosing personal data and document these reasons.

(b) Policies

Organisations should develop and document internal policies that address obligations under the Ordinance. These policies should be made available to employees who should be reminded of these policies and any updates periodically.

Organisations will wish to develop internal policies that give effect to the six data protection principles in the Ordinance. These policies should be documented and should show how they connect to the legal requirements.

The key policies that organisations should have in place are the following:

- Collection of personal data;
- Accuracy and retention of personal data;
- Use of personal data including the requirements for consent;
- Security of personal data;
- Transparency of organisations' personal data policies and practices; and
- Access to and correction of personal data.

Organisations should also incorporate personal data compliance requirements in other policies of the organisation, as appropriate. For example, in contract management policies, procurement policies, human resources policies and policies dealing with the disclosure of personal data to regulatory bodies, law enforcement agencies and other government bodies.

Organisations are advised to refer to the guidance notes issued by the Commissioner on various subjects of data protection.

(c) Risk Assessment Tools

Personal data risks evolve over time. Conducting periodic risk assessments, in particular when there is material change to the regulatory requirements relating to personal data or before making any material change to the data user's existing personal data process or introducing a new personal data process, is an important part of any ***privacy management programme*** *to ensure that the policies and practices of organisations are and remain compliant with the Ordinance.*

Sometimes organisations offer services which collect, use or disclose personal data but which have not been thoroughly vetted from a privacy perspective. Proper use of risk assessment tools can help prevent problems. Fixing a personal data problem after the fact can be costly so careful consideration of the purposes for a particular initiative, product or service, and an assessment that minimises any personal data impacts beforehand is vital.

As a result, such assessments should be conducted throughout the organisation for all new projects involving personal data and on any new collection, use or disclosure of personal data in ways that are materially different from existing practice. Organisations should develop a process for identifying and mitigating leakage and security risks, which could include the use of privacy impact assessments. The Data Protection Officer should play an advisory or consultative role. The Information Leaflet "*Privacy Impact Assessments*"[1] issued by this Office provides assistance in this regard.

(d) Training and Education Requirements

A sound ***privacy management programme*** *requires all relevant members (i.e. those handling personal data) of an organisation to be aware of, and be ready to act on personal data protection obligations. Up-to-date training and education requirements for all relevant employees, tailored to specific needs, are key to an effective* ***privacy management programme****.*

In order for a **privacy management programme** to be effective, relevant employees should be made aware of personal data protection generally and to be conversant with the organisations' policies and practices for compliance with the requirements under the Ordinance. Those who handle personal data directly may need additional training specifically tailored to their roles. Training and education need to be current and relevant. To facilitate this, attending this Office's professional workshops and arranging in-house train-the-trainer programmes would be helpful.

Employees will be able to better protect personal data when they are able to recognise a matter as one that involves personal data protection. Organisations may have very sound policies and programme controls in place but if employees do not follow them, the **privacy management programme** has broken down. Relevant employees should be reminded to comply with the organisation's policies and programme controls as an integral part of their duties.

There are many ways for organisations to deliver training and general personal data protection education. Examples include providing mandatory training modules on the company intranet, small group sessions, one-on-one training, monthly e-newsletters, or inserting modules within training on organisation policies. The organisation should document its training processes and measure participation and success.

---

[1] www.pcpd.org.hk/english/publications/files/PIAleaflet_e.pdf

For personal data protection training and education to be effective, it should:

- be given to new employees in its induction programme and periodically thereafter;
- cover the policies and procedures established by the organisation;
- be delivered in an appropriate and effective manner, based on organisational needs; and
- circulate essential information to relevant employees as soon as practical if an urgent need arises.

(e) Breach Handling

Personal data breaches are expensive on many fronts and taxing on consumer trust.

Organisations should have a procedure in place and an officer or a designated team responsible for managing a personal data breach. Responsibilities for internal and external reporting of the breach should be clear.

While reporting of major data breach to the Commissioner is not mandatory under the Ordinance, the Commissioner encourages organisations to adopt a procedure of notification in handling a data breach.

In handling personal data breach, organisations should consider the circumstances of the breach, and decide whether any of the following persons should be notified as soon as practicable:

- the affected data subjects;
- the law enforcement agencies;
- the Commissioner;
- any relevant regulators; and
- such other parties who may be able to take remedial actions to protect the personal data privacy and the interest of the data subjects affected (for example, Internet search companies may assist to remove relevant cached link from its search engine).

"Guidance on Data Breach Handling and the Giving of Data Breach Notifications"[2] issued by this Office provides practical guidance in this regard.

(f) Data Processor Management

Personal data handling by data processor is another key area to consider. Are there contractual or any other means in place to protect the personal data?

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

- 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 (absolute or qualified) against sub-contracting to other service provider;
- reporting of irregularity;
- measures to ensure contract staff's compliance with the agreed obligations;
- organisation's right to audit and inspect; and
- consequences for violation of the contract.

Organisations are advised to take note of the Information Leaflet *"Outsourcing the Processing of Personal Data to Data Processors"*[3] issued by this Office.

[2] www.pcpd.org.hk/english/publications/files/DataBreachHandling_e.pdf
[3] www.pcpd.org.hk/english/publications/files/dataprocessors_e.pdf

(g) Communication

Organisations should take all practical steps to ensure employees and customers can ascertain their personal data policies and practices.

This communication should be clear and easily understandable and not simply a reiteration of the Ordinance. In general, it should:

- provide enough information so that the public knows the purpose of the collection, use and disclosure of personal data and how long it is retained;
- include information on who to contact with questions or concerns; and
- be made easily available to individuals.

Individuals should be made aware of their ability to access their personal data held by the organisation, and how to request correction or to enquire about the organisations' compliance with the Ordinance.

Part B – Ongoing Assessment and Revision

Part A describes the components for creating a **privacy management programme**. Part B of this Guide outlines the basic tasks involved in the maintenance of a **privacy management programme** to ensure ongoing effectiveness, compliance and accountability. In order to properly protect personal data and meet legal obligations, organisations should monitor, assess and revise their framework to ensure it remains relevant and effective.

1 Develop an Oversight and Review Plan

*An oversight and review plan will help the organisation keep its **privacy management programme** on track and up to date.*

The Data Protection Officer or Data Protection Office should develop an oversight and review plan on a periodic basis that sets out how and when the effectiveness of the **privacy management programme** will be monitored and assessed, as outlined in organisational commitments. Depending on the organisation's compliance and control infrastructure, such plan may be covered in its overall oversight and review system. The plan should establish performance measures and include a schedule of when the policies and other programme controls will be reviewed.

2 Assess and Revise Programme Controls

The effectiveness of programme controls should be monitored, periodically audited, and where necessary, revised.

Monitoring is an ongoing process and should at least address the following questions:

- what are the latest threats and risks?
- are the programme controls addressing new threats and reflecting the latest complaint or audit findings, or guidance of the Commissioner?
- are new services being offered that involve increased collection, use or disclosure of personal data?
- is training necessary and if yes, is it taking place, is it effective, are policies and procedures being followed, and is the programme up to date?

If problems are found during the monitoring process, concerns will need to be documented and addressed by the appropriate officers. Critical issues should be brought to the attention of top management.

For critical or high-risk processes, periodic internal or external audits are important ways to assess the effectiveness of an organisation's **privacy management programme**. Otherwise, it is recommended that the Data Protection Office should conduct periodic assessments to ensure key processes are being respected. For smaller organisations or for less formal reviews, organisations should develop checklists that are reviewed on a regular basis. Through whatever means appropriate, organisations need to put in place practical measures to ensure that employees or contractors are following the organisation's policies and programme controls.

As stated, this document is not a "one-size-fits-all" solution. Each organisation will need to decide how to structure its own **privacy management programme**, taking into consideration a number of factors, including the size of the organisation, the nature of business of the organisation, and the amount and sensitivity of the personal data it handles.

Organisation should conduct assessments of its programme controls (as outlined in Part A) in a focused, continuous and thorough manner.

Based on the results of the assessment process, the Data Protection Officer should consider whether to take action to update and revise the programme controls. This is a critical responsibility. The changes should be communicated to employees either as they are made or in "refresher" education and training modules, as appropriate.

In short, the following actions should be undertaken by the Data Protection Officer:

- **monitor and update personal data inventory** periodically to keep it current and identify and evaluate new collections, uses and disclosures.
- **review and revise policies** as needed following assessments or audits, in response to a breach or complaint, new guidance, industry-based best practices, or as a result of environmental scans.
- **treat privacy impact assessments and security threat and risk assessments as evergreen documents** so that the privacy and security risks of changes or new initiatives within the organisation are always identified and addressed.
- **review and update training and education** on a periodic basis as a result of ongoing assessments and communicate changes made to programme controls.
- **review and adapt breach and incident management response protocols** to implement best practices or recommendations and lessons learned from post-incident reviews.
- **review and, where necessary, fine-tune** requirements in contracts with data processors.
- **update and clarify, where necessary, communication** explaining personal data policies to the organisation's employees and customers.

Privacy Management Programme – At A Glance

Part A
Baseline Fundamentals

Organisational Commitment

Buy-in from the Top	Data Protection Officer/Office	Reporting
• Top management support is key to a successful **privacy management programme** and essential for privacy-respectful culture	• Role exists and is involved where appropriate in the organisation's decision-making process • Role and responsibilities for monitoring compliance of the Personal Data (Privacy) Ordinance are clearly identified and communicated throughout the organisation • Responsible for the development and implementation of the programme controls and their ongoing assessment and revision • Policy and procedures are in place to incorporate personal data protection into every major function involving the use of personal data	• Reporting mechanisms need to be established, and they need to be reflected in the organisation's programme controls

Programme Controls
The following programme controls are in place:

Personal Data Inventory	Policies	Risk Assessment Tools
• The organisation is able to identify the personal data in its custody or control • The organisation is able to identify the reasons for the collection, use and disclosure of the personal data	Covering: • Collection of personal data • Accuracy and retention of personal data • Use of personal data including the requirements of consent • Security of personal data • Transparency of organisations' personal data policies and practices • Access to and correction of personal data	Training & Education Requirements Breach Handling Data Processor Management Communication

Part B
Ongoing Assessment and Revision

Oversight & Review Plan

- Develop an oversight and review plan

  Data Protection Officer or Data Protection Office should develop an oversight and review plan on a periodic basis that sets out how the effectiveness of the organisation's programme controls will be monitored and assessed.

Assess & Revise Programme Controls Where Necessary

- Update personal data inventory
- Revise policies
- Treat risk assessment tools as evergreen
- Update training and education
- Adapt breach and incident response protocols
- Fine-tune data processor management
- Improve communication

Privacy Management Programme

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

www.pcpd.org.hk/pmp

Acknowledgement

This Guide is modelled on "Getting Accountability Right with a Privacy Management Program" (April 2012), available at www.oipc.bc.ca/guidance-documents/1435 compiled by the Office of the Privacy Commissioner of Canada, and the Offices of the Information & Privacy Commissioners of Alberta and British Columbia, Canada, by courtesy of the authors.

Disclaimer

The information provided in this Guide is for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance. For a complete and definitive statement of law, direct reference should be made to the Ordinance itself. The Commissioner makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the above information. The above suggestions will not affect the functions and power conferred to the Commissioner under the Ordinance.

Office of the Privacy Commissioner for Personal Data, Hong Kong

Enquiry Hotline : (852) 2827 2827
Fax : (852) 2877 7026
Address : 12/F, 248 Queen's Road East, Wanchai, Hong Kong
Website : www.pcpd.org.hk
Email : enquiry@pcpd.org.hk

First published in February 2014