A PRACTICAL GUIDE FOR

IT MANAGERS AND PROFESSIONALS ON THE PERSONAL DATA (PRIVACY) ORDINANCE

Published by:

HONG KONG COMPUTER SOCIETY

Supported by:

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

Table of Contents

FOREWORD

The pervasive use of new information and communications technologies in today's digital society has enabled the collection, storing and mining of vast amounts of personal data with phenomenal ease and efficiency. The resultant opportunities are immense, involving the creation of economic and societal values, and enhancement of the productivity and competitiveness of enterprises in ways previously beyond our imagination. At the same time, they also pose grave risks to privacy and raise serious concerns about the protection of personal data.

The Personal Data (Privacy) Ordinance was enacted in December 1996. Despite the impact of new and rapidly evolving technologies in the interim, the fundamental principles of privacy and data protection, as enshrined in the six Data Protection Principles (DPPs) of the existing legislation, have stood the test of time and remain relevant. To achieve enduring organizational success, it is important that corporate data users and their service providers are fully aware of these principles and the privacy implications of the technologies they are adopting. More specifically, the six DPPs have to be embedded in all of the enterprise's organizational processes and information systems.

To this end, the Hong Kong Computer Society has compiled this practical guide for IT managers and professionals. I salute them on this great initiative as it contributes to building a trustworthy and privacy-assuring digital ecosystem. Among other things, the guide provides a landmark review of a comprehensive range of IT and technology applications in relation to protection of personal data privacy, and offers practical guidance for compliance with the six DPPs. This sector-specific effort is the first of its kind and I hope it will serve as an example for many other sectors to follow.

Allan Chiang
Privacy Commissioner for Personal Data

PREFACE

The Hong Kong Computer Society (HKCS), as a professional body in IT, has the mission of IT talent cultivation and professional development. The Society encourages our youngsters to study IT related courses in our tertiary institutions and to adopt ICT as a career. For IT professionals, the Society provides a platform for continual and relevant knowledge enhancement through conferences, Special Interest Groups (SIG) seminars and ad-hoc knowledge-based events and projects.

The rapid and sophisticated advances in IT have led to the proliferation of e-services including e-commerce, social networks and personalized services e.g. e-banking, with such services necessitating the collection, use and disclosure of personal data to fulfill the purposes intended. With major concerns on privacy intrusion risen from unauthorized or fraudulent use of personal data as well as data breaches, governments have introduced data privacy laws, including Hong Kong which enacted the Personal Data (Privacy) Ordinance in 1996 and established the Office of the Privacy Commissioner for Personal Data (PCPD) to promote and enforce the PD (P) O.

To enhance the understanding of and thereby effective compliance with the PD (P) O for IT managers and practitioners, the HKCS, assisted by the Office of the Privacy Commissioner for Personal Data, has developed a practical Guide for IT managers and professionals on the requirements under PD (P) O covering the six data protection principles as well as certain selected areas of direct relevance to the IT industry.

The Working Group, composed of experts in various and relevant fields, was set up in 2011 dedicated to the production of this informative document. As the Convenor of this Working Group, I wish to acknowledge its Members for their tremendous efforts and contributions:

Mr John Chiu, JP, Managing Director, AT Group Limited
Mr Dennis Fullgrabe, Chief Internal Auditor, Hospital Authority
Mr Thomas Parenty, Managing Director, Parenty Consulting Limited
Ms Susanna Shen, CIO, The Hong Kong and China Gas Company Limited
Mr Peter Yan, Executive Director, Computer And Technologies Holdings Limited
Professor Y B Yeung, Adjunct Professor, Department of Information Systems, City University of Hong Kong

and to our advisor, Henry Chang, IT Advisor to the PCPD, for his valued views and for his coordination of relevant colleagues at the Office of the PCPD in contributing to and reviewing the Guide.

Stephen Lau, JP
President
Hong Kong Computer Society

Chapter 1
Introduction

1.1 The advent of computers has contributed much to data privacy concerns, in particular personal data privacy. As early as 1975, in a UK Government's white paper, which led to the first law in the UK to protect personal data privacy, the following observations were made on computers:

(a) they facilitate the maintenance of extensive record systems and the retention of data in those systems;

(b) they can make the data easily and quickly accessible from many different points;

(c) they make it possible for data to be transferred quickly from one information system to another;

(d) they make it possible for data to be combined in ways which might not otherwise be practicable; and

(e) because the data are stored, processed and often transmitted in a form which is not directly intelligible, few people may know what is in the record or what is happening to it.

1.2 With the sophisticated advance in computer and telecommunications technologies in the 80's, the Internet going critical in number of users and the advent of e-commerce in the 90's, together with the phenomenal growth of social media and mobile technology users in the 2000's, personal data privacy is now a global issue. High-profile data breaches of millions of sensitive personal data including financial and health records, and corporate use of personal data for purposes other than the original purpose of data collection are two pervasive examples of personal data intrusion which have led to the promulgation of laws aiming to protect personal data of individuals in many countries.

1.3 In 1995, Hong Kong enacted the Personal Data (Privacy) Ordinance (PD(P)O), to protect the personal data privacy of individuals, with six data protection principles (DPPs) governing the proper collection, accuracy, retention, use, security, access and correction of personal data in both the public and private sectors. The independent Office of the Privacy Commissioner for Personal data (PCPD) was established in 1996 with the mandate to promote good data protection practices and to oversee data users' compliance with PD(P)O.

1.4 Since its establishment, PCPD has issued guidance to data users on different areas to promote good data protection practices. This guidance document is initiated by the Hong Kong Computer Society and assisted by PCPD to provide a practical guide for IT managers and professionals on the requirements under PD(P)O covering the six data protection principles as well as certain selected areas of direct relevance to the IT industry.

1.5 Chapter 2 of this document outlines the definitions of various terms used in the whole document. The next chapter then discusses personal data protection on an enterprise level, that it becomes a key to good corporate governance, accountability and transparency. Compliance with PD(P)O and good governance on respecting personal data privacy of customers and employees require the establishment of a clear and enterprise-level personal data protection policy which demonstrates top management commitment and also provides relevant rules for the enterprise to follow. Ingraining a privacy protection culture within the enterprise, where personal data protection is second nature, is key to fulfilling the objectives of legal compliance as well as building up customers' trust and confidence in the enterprise.

1.6 A systemic process, Privacy Impact Assessment (PIA), is strongly recommended to be undertaken to identify any privacy risks and issues before launching or revising any major projects involving personal data. In Chapter 4, guidance is offered on the types of projects as likely candidates for PIA, when it should be conducted, how to conduct it, the risk analysis as well as measures for mitigating privacy risks.

1.7 In today's world, it is most often not a case of "IF" an enterprise will have a data privacy breach, it is more a case of "WHEN". A data privacy breach can result in your organisation getting the adverse attention of news media and industry regulatory agencies, not to mention the enterprise's customers and employees. Chapter 5 provides guidance on the establishment of an effective Incident Response Strategy, which deals with the classification and discovery for data breach incidents, and the subsequent report, containment, investigation and recovery of such incidents.

1.8 Chapter 6 offers practical guidance on the application of the six DPPs in system design, development and operations. It gives an overview of the six DPPs and provides reader-friendly guidance for data users to follow in the design and operations of IT applications. In particular, the section on the security principle, DPP4, offers very detailed guidance on security protection measures across the entire spectrum of data collection, retention, storage, transmission and use of personal data.

1.9 The final chapter provides practical guidance on major topics related to IT and technology applications, including outsourcing and cloud computing, workplace monitoring, direct marketing and biometric applications. These selected IT-intensive applications, which could be highly privacy intrusive, are increasingly pervasive in their use. Guidance is offered to ensure compliance with the data protection principles while attaining the underlying objectives of undertaking such applications.

Chapter 2
Definitions

Various Definitions

2.1 The definition of the term "**data**" is provided in **section 2(1)** of PD(P)O as follows:
" 'data' means any representation of information (including an expression of opinion) in any document, and includes a personal identifier."

2.2 The term "**document**" is in turn defined in **section 2(1)** as follows:
" 'document' includes, in addition to a document in writing –
(a) a disc, tape or other device in which data other than visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the disc, tape or other device; and
(b) a film, tape or other device in which visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the film, tape or other device."

2.3 Therefore for any information to constitute "data" under PD(P)O, such information must have been recorded in a "document".

2.4 The definition of the term "**personal data**" is given in **section 2(1)** of PD(P)O as follows:
" '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."

2.5 A totality concept or approach is taken by the Privacy Commissioner in establishing whether certain data constitute personal data. For example, a residential address, say "1234 Harbour Road" just on its own does not constitute personal data; but if it is coupled with a name, say Mr Chan Tai Man, in a document e.g. an application form, "No. 1234 Harbour Road" does constitute the personal data of Mr Chan Tai Man. Therefore generally speaking, if it is practicable to ascertain from the totality of data the identity of the individual, then each and every part of the data constitutes the personal data of the individual.

2.6 There are frequent questions related to a number of technology-related information items, which are discussed below.

Is an Email Address Personal Data?

2.7 Email address, in some circumstances, could be information from which the identity of an individual may be directly or indirectly ascertained, e.g. Chan.tai.man@abc.com. Using the totality approach, if an email address is associated or coupled with a named person, say Mr Chan Tai Man who works in abc company, the email address does constitute the personal data of Mr Chan Tai Man.

However, just the email address on its own, in the absence of any other associated data, does not constitute personal data. This is based on a decision by the Administrative Appeals Board (AAB) that the email address "huoyan_1989" was not the complainant's name and was not the complainant's personal data.[1]

2.8 In another case, the AAB did not accept that an email address which corresponded to the initials of a complainant was sufficient to lead to the conclusion that the complainant's identity would become reasonably ascertainable from such an address, and therefore the email address in question was not the complainant's personal data[2].

Is IP Address Personal Data?

2.9 IP address is a specific machine address assigned by the Internet Service Provider to a user's computer and is therefore unique to a specific computer. In an AAB case[3], the Privacy Commissioner received a complaint relating to the disclosure of information, including an IP address of a computer that disseminated the information. The Privacy Commissioner viewed that an IP address was information about an inanimate computer, not an individual. It did not contain information that "relates" to an individual. Further, it was noted that an IP address alone could not reveal the identity of the computer user, and thus lacking the characteristic of identifying an individual directly or indirectly. However, in certain circumstances IP address can constitute "personal data" when it is read together with other information, provided that the identity of an individual can be ascertained. The AAB agreed that, in the circumstance of that particular case, the information together with the IP address disclosed did not amount to personal data of the complainant. It further mentioned that when IP address was coupled with such verified personal information as names, identity card numbers and addresses, it would, indeed, constitute "personal data".

2.10 Two other definitions are of particular relevance to this guidance document.

Data User

2.11 The term "**data user**" is defined in **section 2(1)** of PD(P)O as follows:

> *" 'Data user', in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data."*

2.12 Another point worth noting regarding the meaning of "data user" is the exclusion under section 2(12), which provides:

> *"A person is not a data user in relation to any personal data which the person holds, processes or uses solely on behalf of another person if, but only if, that first-mentioned person does not hold, process or use, as the case may be, those data for any of his own purposes."*

[1] AAB No. 16/2007
[2] AAB No. 25/2008
[3] AAB No. 16/2007

2.13 To understand this provision, a good example is the case of the internet service provider (ISP), that by merely providing the means of internet linkage it does not thereby render the ISP a data user especially when it does not control the collection, holding, using or processing of the personal data of individuals accessing and using such online functions as, for example, chat rooms to disseminate and communicate with other users. The ISP is thus to that extent not a data user as excluded under section 2(12).

Data Subject

2.14 The term "**data subject**" is defined in **section 2(1)** as follows:

> *"Data subject, in relation to personal data, means the individual who is the subject of the data."*

Chapter 3

Strategy and Policy for Personal Data Protection at the Enterprise Level

Introduction

3.1 Good privacy practices are a key part of corporate governance and accountability. An organisation is legally obliged to observe the requirements under PD(P)O to protect personal data privacy. It is also good for business as many leading companies nowadays use them to gain competitive advantage through earning the confidence and trust of their customers, business partners and oversight bodies. The aim is to ensure that personal data is protected in any given IT system or business practice. Personal data protection is therefore an enterprise-wide responsibility, and is particularly relevant to IT professionals.

3.2 There are numerous ways and various strategies, usually dependent on the industry and regulatory requirements, that organisations can use to achieve and sustain personal data protection. Preferably these should be pro-active rather than reactive and usually will include these four key elements:

- a clear personal data protection policy that demonstrates top management commitment and strengthens personal data protection governance;
- embedding measures in systems from the outset, using a risk-based approach, that put privacy policies into effect;
- ingraining privacy culture through promotion, education and training; and
- continuous improvement through ongoing monitoring, oversight and assurance reviews.

Clear Personal Data Protection Policy

3.3 Personal data protection governance is underpinned by a clear, enterprise-wide, personal data protection policy that demonstrates top management commitment and also provides rules that the organisation should follow. Such a policy would stress the importance of maintaining the confidentiality, integrity and availability of personal data. It would also explicitly commit the organisation to preserving the security and privacy of the personal data it holds. Generally this would include that:

- all identifiable personal data be accorded the highest level of security and privacy protection in accordance with the requirements under PD(P)O;
- all IT projects involving personal data explicitly take account of the information/privacy policy and the principles established in PD(P)O and conduct a Privacy Impact Assessment before launching;
- all employees, as well as non-employees, who are involved in the handling and processing of personal data, must comply with the policy and should be provided with regular training on personal data protection;
- staff are encouraged to be on the alert for and to report possible security and data breaches; and
- persons responsible for such deliberate violations and breaches may be subject to disciplinary and legal actions.

3.4 The policy should be effectively communicated, especially to new staff and contractors, be easily accessible and be reviewed periodically, particularly in the light of any law revisions or lessons learnt from incidents in your own or other organisations.

Embedding Mechanisms in Systems

3.5 It works best if privacy protection is embedded in the design and architecture of IT systems and business practices, and is not seen as an add-on or an after-thought. Various sections in this guide provide practical advice on how this can be achieved. The result is that privacy protection then becomes an integral component of the functionalities being delivered.

3.6 Regardless of the size, structure or nature of an organisation, the management of personal data unavoidably gives rise to privacy risks. Such risks can be even higher for financial and health information. Embedded mechanisms should aim to prevent such risks from materialising or work to minimise the impact, if they do. It justifies the adoption of a systematic, risk management approach:

- *Identifying Privacy Risks*: Effectively protecting personal data requires identification of potential privacy risks so they can be managed. This can be achieved through both formal (e.g. establishing privacy review committees, conducting PIA) and informal methods (e.g. listening to employees and business partners). If you do not identify it, you cannot manage it.
- *Analysing and Prioritising*: Not all risks warrant the same degree of attention. Determining the inherent risk – that is, the likelihood of a priv acy event occurring multiplied by its potential impact – is the starting point. Naturally, those with the greatest risk are those warranting the highest priority.
- *Treating Risks*: You now need to determine how best to address these identified privacy risks. The most effective privacy risk treatment is one taken before a risk materialises i.e. preventive not remedial. Technological solutions, such as end-point security and encryption, can often provide the most effective treatments. Detective and corrective measures, which can minimise the impact, may also be appropriate.

3.7 Such an approach can also be referred to as a “privacy by design” approach.

Ingraining a Privacy Culture

3.8 Personal data protection is not solely a technical or policy issue – it is also behavioural. Most importantly, risk treatments therefore need to include and be supported by a culture of data privacy protection, where data privacy is “second nature” in day-to-day business, such that data privacy is the default and is a personal responsibility for each staff member. Building and maintaining such a culture within your organisation requires a persistent effort over the long term. These should include:

- a planned and sustained programme to raise awareness of data privacy across the organisation;

- committed leadership from top management, clear articulation of data privacy as an organisational priority, and that they are seen to "walk the talk";
- effective communication of key data privacy, security messages and making relevant guidance readily available;
- third parties, such as IT contractors, confidential waste disposal contractors, among others, who may also have access to or handle personal information, to be brought under the personal data privacy protection regime; and
- continuous update and renewal.

Continuous Improvement

3.9 Monitoring for improvement is always an essential step. Like most complex risks, data privacy risks continuously evolve. Consequently it is necessary to examine strategies on a regular basis to determine whether or not they are achieving the desired outcomes. This would include:

- having early warning and internal measurement devices in place to assure the actions meet the words;
- monitoring trends in privacy incidents and complaints, and inculcating the lessons;
- making regular and visible "walk-arounds" to assess compliance and gain feedback;
- ensuring periodic self-assessment of strategies and performance; and
- conducting independent periodic audits to verify performance.

Useful References

Information and Privacy Commissioner, Ontario, Canada (November 2009), *Privacy by Design: Essential for Organisational Accountability and Strong Business Practices (http://www.privacybydesign.ca/content/uploads/2009/11/2009-11-02-pbd-accountability_HP_CIPL.pdf)*

Information and Privacy Commissioner, Ontario, Canada (April 2010), *Privacy Risk Management (http://www.privacybydesign.ca/content/uploads/2010/07/pbd-priv-risk-mgmt.pdf)*

Chapter 4
Privacy Impact Assessment

What is a Privacy Impact Assessment (PIA)?

4.1 According to the Information Leaflet on PIAs issued by the Privacy Commissioner in July 2010, a PIA "is a systematic process that evaluates a proposal in term of its impact upon personal data privacy with the objective of avoiding or minimising adverse impact". As an integral part of the project planning process, it helps an organisation to:

- identify the potential impact that a proposal may have upon individuals' personal data privacy;
- examine how any detrimental effects upon data privacy might be overcome; and
- ensure that new projects comply with DPPs.

Why Undertake a PIA?

4.2 A PIA offers an early chance to identify any privacy risks and issues before launching any projects or major changes involving personal data. This enables the decision-maker to make an informed decision and to adequately consider the impact on personal data privacy before undertaking the project. These can then be addressed up-front using a "privacy-by-design" approach.

4.3 Additionally, conducting and acting on a PIA report increases the chances that any privacy coverage in the media concerning the organisation is good news for the business rather than a public relations disaster.

Who Should Undertake a PIA?

4.4 PIA is the organisation's responsibility. Ideally, the process should involve or be supported by in-house expert and other relevant staff. An external expert (e.g. data privacy consultant) should be considered for projects with significant data privacy risks.

4.5 Unless people with the right competencies are employed, it is likely that the assessment process will be more difficult and protracted than necessary. The resulting analysis and conclusions may also be less sound or insightful.

Which Projects Warrant a PIA?

4.6 Although not expressly provided for under PD(P)O, a PIA is an important compliance tool. Not every project, however, will need a formal PIA. It will depend on the nature and scope of the project and the volume and nature of the personal data involved.

4.7 Some projects are of such a scale or nature that the need for a formal PIA is evident. For example:

- the proposed electronic health record (eHR), which will hold personal data on a significant proportion of Hong Kong's population;
- the application of cutting edge technology to an aspect of data processing where the effects are not widely understood or trusted by the public such as requiring customers to undergo biometric identification to access a service; and
- where the surveillance capacity or intrusiveness may be of such a nature as to make the merits of a formal PIA seem obvious.

4.8 There will be various other more mundane, but nonetheless significant projects, which will also benefit from a formal PIA. For example:

- centralising a multi-national company's employee records in Hong Kong or elsewhere;
- merging internal business databases to enable new forms of client profiling; and
- changing the way information is collected in customer interface systems (for instance, adopting unattended kiosks, automated voice responses that capture personal data, smartcards).

4.9 Additionally, a formal PIA may be desirable to assess and address potentially higher data privacy risk situations such as:

- arising from a new technology or the convergence of existing technologies (e.g. combining face-recognition and CCTV);
- where a known privacy-intrusive technology is to be used in new circumstances (e.g. installing video surveillance in a workplace); and
- following a major change in practice with significant data privacy effects (e.g. the adoption of new forms of required ID, shared access with other organisations' electronic databases).

When Should a PIA be Undertaken?

4.10 The ability to design system architecture that addresses actual or potential data privacy concerns is dependent, to a certain extent, on early identification of data privacy issues and risks. Ideally, full and detailed consideration of data privacy issues should precede system design and preferably be conducted before the project is commenced to ensure data privacy risks and issues are identified early and before decisions are set in stone.

4.11 However, sometimes it may only be possible to complete a PIA at later stages in the system development and acquisition phase. If so, the PIA report can be an evolving document which will become more detailed over time.

How is a PIA Conducted?

4.12 There is no one-size-fits-all PIA model. The PIA process may vary depending upon the organisational structure, size and process environment, or project nature, but would generally include the following key stages:

- data processing cycle analysis;
- privacy risk analysis;
- avoiding or measures for mitigating privacy risks; and
- PIA reporting.

Data Processing Cycle Analysis

4.13 This entails a critical examination of the purpose and whether it is necessary to collect the kind, amount and extent of personal data contemplated. Practically speaking, the less sensitive the data collected, the lower the potential impact on data privacy.

4.14 A typical list of matters to be addressed would include, but not be limited to, the following:

Purpose *(DPP1)*	The purpose for which and the circumstances under which the personal data are collected. Are there less privacy intrusive alternatives?
Accountability	The roles and responsibilities of owner, developer, system maintenance personnel, custodian and users of the personal data.
Choice & Consent *(DPP1)*	The choice of acceptance, declination, alternatives and consent to be obtained from the data subject for data collection.
Collection Limitation *(DPP1)*	How the personal data is to be collected - the collection of personal data should be necessary for or directly related to the collection purpose plus the data should be adequate for but not exceed the purpose.
Use & Processing *(DPP3)*	How the personal data is to be used and processed, including transfer and sharing. Also, what are the criteria under which personal data can be shared and disclosed to third parties.
Retention & Accuracy *(DPP2)*	The policy regarding the appropriate retention period and steps to be taken to make sure that personal data collected, used or disclosed is accurate, complete and up-to-date.
Access & Correction *(DPP6)*	How and by whom the personal data can be accessed and the ways to enable correction.
Security Protection *(DPP4)*	The security safeguards to prevent unauthorised or accidental access, use, modification or loss of personal data, including all interfaces, links and transmissions to other applications and systems.
Compliance *(DPP5)*	The privacy policy and practices to be devised and made generally available; and should include monitoring and compliance with DPPs.

Privacy Risk Analysis

4.15 Identify and analyse how the project/change impacts upon data privacy. In analysing the data privacy risks, the relevant factors that should be taken into account would include:

- the functions and activities of the data users;
- the nature of the personal data involved and the number of individuals affected;
- the gravity of harm that may be caused to the data subjects should there be improper handling of their personal data; and
- the privacy standards and rules prescribed under applicable codes of practice, guidelines, policies and regulations that the organisation shall observe, etc.

Avoiding or Mitigating Privacy Risks

4.16 Once the privacy risks have been identified and analysed, you need to consider what practical actions may be taken to reduce each risk to an acceptable level. It is highly advisable that a "privacy-by-design" approach be adopted and privacy enhancement technologies be considered and used in the design stage of the personal data system. At this stage there is a need to identify appropriate measures to avoid and/or to mitigate the privacy risks.

4.17 **Avoidance** measures are means to dissipate a privacy risk. It refers to decision criteria in order to avoid the particular privacy risks arising and can include, for example:

- minimising the collection of personal data to only that which is strictly necessary to fulfil the objectives of the project;
- non-collection of contentious data-items; and
- active measures to stop or block the use of particular personal data in decision making.

4.18 **Mitigation** measures are features that may positively compensate, either wholly or partially, for other privacy intrusive aspects of a design, and can include, for example:

- safely and completely deleting and erasing personal data when it is no longer required for the purpose;
- defining clearly and limiting the number of persons who can access and use the personal data on a "need-to-know" basis;
- incorporating an appropriate level of security measures into the design so that confidentiality, integrity and accountability can be achieved; and
- establishing logging and reporting mechanisms to detect and notify appropriate parties in the event of a data breach.

PIA Reporting

4.19 The PIA report records the due process undertaken by an organisation to proactively manage the privacy risks. A typical PIA report needs to cover the following common elements stemming from the previous sections:

A. Introduction and overview.
B. Description of the project and information flows.
C. Data processing cycle analysis highlighting the circumstances and extent of:
   - Personal data collection; and
   - Use, disclosure and retention of the personal data.
D. Privacy risk identification analysis.
E. Avoiding or measures for addressing the data privacy risks by:
   - Planned or proposed privacy enhancing responses;
   - Explanation in sufficient details on how the less privacy intrusive alternatives have been considered and where appropriate, why they are adopted or rejected; and
   - Compliance / monitoring mechanisms.
F. Conclusions.

4.20 Consider updating the PIA report if there are significant changes later on.

Do PIA Reports Need to be Submitted to the Privacy Commissioner?

4.21 It is not mandatory to submit a PIA report to the Privacy Commissioner upon its completion. However, while the Privacy Commissioner neither endorses nor approves PIA reports submitted to him because of the potential conflict with his regulatory role, he may offer comments on matters considered in the report, such as the privacy risk analysis undertaken if the matters involved attract significant privacy concerns.

Useful References

Office of the Privacy Commissioner for Personal Data, Hong Kong (July 2010), *Information leaflet: Privacy Impact Assessments*
(http://www.pcpd.org.hk/english/publications/files/PIAleaflet_e.pdf)

Privacy Commissioner of New Zealand (June 2007), *Privacy Impact Assessment Handbook*
(http://privacy.org.nz/assets/Files/Brochures-and-pamphlets-and-pubs/48638065.pdf)

Chapter 5
Data Breaches and Privacy Incident Management

Why is a Data Privacy Incident Strategy Necessary?

5.1 In today's world, it is most often not a case of "IF" an organisation will have a data privacy breach, it is more a case of "WHEN". This recognises that no safeguards can provide absolute and total protection all of the time. Any data privacy breach can result in your organisation getting the attention of news media and industry regulatory agencies, not to mention your organisation's customers.

5.2 How your organisation responds to and handles a data privacy incident can have a dramatic impact financially and on public image. An incident management strategy is therefore necessary to ensure a quick, effective and orderly response to an unforeseen data privacy incident. It can also help reduce any initial "panic reactions" and "knee-jerk decisions" when the organisation discovers it has had such an incident.

Who Should be Responsible for the Incident Response Strategy?

5.3 Establishing a successful data privacy incident response capability requires substantial planning and resources. Ideally, this would include an Incident Response Team (IRT), made up of appropriately skilled and trusted members of the organisation with senior level participation, which would handle data privacy breach incidents throughout their lifecycles from occurrence, response, rectification and prevention. At times the IRT may be supplemented by external experts.

5.4 The IRT is responsible for co-ordination and oversight of the data breach incident response strategy. This would include deciding upfront what services the IRT should provide, which team structures and models can best provide those services, and selection and implementation of one or more IRTs as appropriate for the organisation's environment. These teams could include, for example, permanent members, such as the privacy officer and IT security specialists, and virtual members, normally consisting of business managers, communications/public relations, human resources, or other security groups. The IRT's roles and responsibilities should be established in a formal terms of reference approved by top management, and providing explicit decision-making authority for facilitating the incident response process.

5.5 When notified of a data privacy incident, the privacy officer should assemble the IRT as appropriate to the nature of the incident and composition determined by the facts and circumstances of the individual incident, as known. Other virtual members, such as forensic experts, should be added as and when the circumstances arise.

What Does an Incident Response Strategy Involve?

5.6 An incident management strategy would generally include the following phases:
- discover and classify incidents;
- report, contain, investigate and recover; and
- post-incident review.

Discover and Classify Data Privacy Incidents

5.7 ***Discovery*** involves both reactive and proactive processes that gather, monitor or receive potential incident information from internal and external sources as well as from monitoring for indications with tools like intrusion detection systems (IDS).

5.8 Encourage staff to report data privacy incidents in a timely manner by:
- stating clearly the importance and the need for timely reporting;
- embedding a reporting culture through policy implementation and education;
- establishing a just culture – one where people will not automatically be blamed; and
- providing an avenue for reporting.

5.9 ***Classify*** the nature of the data privacy incident:
- determine the nature of the incident: whether it is due to crime related activities such as theft, hacking, fraud etc.; or due to accidents such as loss in transit, improper disposal, etc.;
- conduct a quick triage to classify, prioritise, and validate the initial information; involve responsible management in complex cases; and
- preserve evidence and begin documentation of the incident.

Report, Contain, Investigate and Recover

5.10 ***Report*** incidents in a planned and effective manner. The reporting mechanism should enable a fast escalation to senior management. The incident details reported should include:
- general description of what occurred;
- when it happened - date and time;
- place of breach;
- how it occurred, and whether it is one-off or still occurring;
- who detected the breach and how;
- the type of personal data leaked in the breach (HKID, date of birth, contact address, phone number, etc.);
- number and identity of person(s) whose personal data were involved in the breach; and
- where appropriate, remedial / containment actions taken.

5.11 With the declaration of a privacy incident, an IRT specific for the incident would be assembled and assume coordination of the incident response, and this team would produce an immediate action plan and start identifying further information about the actual data involved:

- source and data owner, IT systems involved;
- estimated volume of personal data involved (e.g. 5,000 records);
- age of data involved/time period covered (e.g. 1 year old, 4-5 years ago);
- any protection that was/may still be in place (e.g. data encryption);
- what jurisdictions are involved;
- who already has knowledge of the incident (e.g. media already know); and
- whether external consultants will be required (e.g. legal counsel, public relations firm, investigative or forensic services).

5.12 ***Contain*** the damage. Privacy incidents not only impact on the affected individuals but they can also undermine the trustworthiness of the organisation. These could lead to further governance issues if they are not handled carefully. Assessment of impacts and containment measures are essential:

- assess the impacts on the organisation and the individual(s), e.g. estimate the risk and probability that the breach will result in an identity theft of the affected individuals;
- immediately suspend the system / server if the data breach is caused by system failure or hacking;
- timely, accurate and appropriate communications internally and possibly externally (e.g. the Privacy Commissioner, regulators, law enforcement agencies, customers and the media) on the response plan of the organisation to the incident;
- take actions to respond to and reduce the impacts and deliver, if applicable, immediate interim measures to prevent reoccurrence. These could include:
    - limiting who represents or speaks for the organisation about the incident;
    - containing rumours as much as possible;
    - providing call centre staff with scripts and training to respond to calls;
    - securing data processing operations to prevent further disclosure of information, e.g. upgrading systems with patches or installing additional monitoring;
    - taking measures, such as change of users' passwords and system configurations, to control access as required; and
    - seeking technical assistance internally or outside as appropriate.
- take actions necessary to secure evidence, as required; and
- if the situation worsens, activate planned escalation measures.

5.13 ***Investigate*** and assess the root causes and risk mitigation options to address them. This is an important step towards the longer term protection measures. An organisation needs to learn from lessons such as how the incident has happened and the reasons for failure of the existing controls, thus helping the development of future protection measures.

5.14 ***Recover*** business operations, if applicable. Business operations may experience interruptions when a data privacy incident occurs; the extent will depend on the nature of the business and the incident. Planned recovery actions will be crucial to resume the business operations in an orderly manner. Recovery is usually accompanied with short term mitigation or long term protection measures.

Post-Incident Review

5.15 One goal of the post-incident review should be the development of a final report that documents the entire incident and includes a detailed timeline of events, a formal documentation of decisions made and a log of all incident-related data.

5.16 Another goal is learning the lessons for improving the management of such incidents in future. It is emphasised that data privacy incident management processes are iterative, constantly changing and adapting to better identify, respond to and maybe even prevent new threats. Rarely will there be an incident from which an organisation or a response team will not be able to learn something. For example, necessary changes to procedures will likely be identified.

Does the Incident Need to be Reported to PCPD?

5.17 It is not a mandatory requirement under PD(P)O for organisations to report actual or potential privacy breaches to PCPD. However, PCPD encourages organisations to do so voluntarily. Organisations that do so will generally receive practical advice from PCPD to remedy the breaches and be much better prepared to respond to questions from the public, the media, etc.

Do Affected Individuals Need to be Notified?

5.18 Notification of affected individuals should occur if it is believed to be necessary to avoid, mitigate or address harm to them. Some considerations in determining whether to notify and what information to provide to individuals affected by the breach include:

- policy or relevant regulations that require notification;
- contractual obligations that require notification;
- public expectation;
- risk of identity theft or fraud;
- risk of harm, stalking or harassment of the data subjects; and
- risk of hurt, humiliation or damage to the data subjects.

5.19 This notification could typically provide:

- detailed information about the breach including what type and form of information was involved in the breach (as appropriate given any possible law enforcement investigation in progress);
- steps taken to prevent it from happening again;
- how the individual whose data was involved may be impacted;
- identification of any steps the individual may have to take to protect himself or herself;
- what the organisation is doing for the individual; and
- who to contact with questions or for more information.

5.20 This notification to the affected individuals should be considered as a high priority to enable them to take appropriate precautionary measures against the possible impact on themselves.

5.21 Having assessed the situation and the impact of data breach, this notification should be made as soon as practicable after the detection of the breach, except where law enforcement agencies have, for investigation purposes, made a request for a delay.

Post-Incident Follow-up

5.22 As soon as all the steps associated with containing and handling the incident are completed or are underway, the organisation should look into the root cause of the incident and where appropriate, develop means or improve existing steps to prevent a similar incident from happening again.

Useful References

Office of the Privacy Commissioner for Personal Data, Hong Kong (June 2010), *Guidance Note on Data Breach Handling and the Giving of Breach Notifications (http://www.pcpd.org.hk/english/publications/files/DataBreachHandling_e.pdf)*

Internal Organisation for Standardization (ISO) (2004), *ISO 18044:2004 - Information technology - Security techniques - Information security incident management*

Dana, W.L. (2007), Does Your Organisation Have A Privacy Incident Response Plan? (https://isaca-washdc.sharepointsite.net/resources/Articles/article-may2007-print.htm)

National Institute for Standards and Technology (March 2008), *Computer Security Incident Handling Guide, Special Publication 800-61, Revision 1 (http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf)*

Chapter 6
Practical Guidelines on the Application of the Six Data Protection Principles (DPPs) in Systems Design, Development and Operations

The Six DPPs

6.1 DPP1 - Purpose and Manner of Collection of Personal Data

(1) Personal data shall not be collected unless-
- (a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
- (b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and
- (c) the data are adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are-
- (a) lawful; and
- (b) fair in the circumstances of the case.

(3) Where the person from whom personal data are or are to be collected is the data subject, all practicable steps shall be taken to ensure that-
- (a) he is explicitly or implicitly informed, on or before collecting the data, of-
  - (i) whether it is obligatory or voluntary for him to supply the data; and
  - (ii) where it is obligatory for him to supply the data, the conse quences for him if he fails to supply the data; and
- (b) he is explicitly informed-
  - (i) on or before collecting the data, of-
    - (A) the purpose (in general or specific terms) for which the data are to be used; and
    - (B) the classes of persons to whom the data may be transferred; and
  - (ii) on or before first use of the data for the purpose for which they were collected, of-
    - (A) his rights to request access to and to request the cor rection of the data; and
    - (B) the name and address of the individual to whom any such request may be made,

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of PD(P) O as a purpose in relation to which personal data are exempt from the provisions of data protection principle 6.

The Essence of DPP1

6.1.1 **Only necessary, adequate but not excessive personal data are to be collected for a lawful purpose directly related to a function or activity of the data user.** For example, to open an account with a bank, the bank should only collect from the prospective client personal data related to the purpose of opening and maintaining the client's account.

6.1.2 Given the complexity of modern business transactions and technological advances such as data mining, data users are tempted to collect a broad variety of personal data which are seemingly not necessarily related to the specific purpose of data collection but just in case that they might be useful at some point in the future. Data users have to consider carefully the purpose of collection because the data collected should not be excessive in relation to the collection purpose. For sensitive personal data, such as identity card number, it is essential to consider seriously whether there is any actual need for their collection.

6.1.3 Generally speaking, before the collection of any personal data, due consideration should be given to relevant factors, such as:

- the particular function or activity to which the collection of the data concerned is considered directly related;
- the degree of sensitivity of such data;
- the legitimate purposes to be served in collecting the personal data and the adverse impact on personal data privacy;
- whether there is a real need (i.e. the degree of likelihood of such need arising) for the data to be collected in order to carry out that function or activity;
- whether there is any realistic and less privacy intrusive alternative for attaining the purpose of collection.

6.1.4 Specifically, for a number of specific industries and fields of activity, three Codes of Practice have been issued by the Privacy Commissioner to provide useful reference on personal data which may be collected:

a. Code of Practice on the Identity Card Number and Other Personal Identifiers;
b. Code of Practice on Consumer Credit Data; and
c. Code of Practice on Human Resource Management.

6.1.5 **The collection of personal data should be lawful and fair.** In stating the obvious, the means of data collection is unlawful if it is prohibited under the law. The theft of someone else's credit card or bank account information is a good example of collection by unlawful means.

6.1.6 Examples of unfair collection of personal data include the use of blind advertisement for fictitious job positions to obtain applicants' resume in order to use their personal data for other purposes including direct marketing. It should also be noted that, generally speaking, the use of covert video recording as a means of capturing an individual's personal data without his or her knowledge or consent is highly privacy intrusive and might amount to unfair collection of personal data of the targeted data subject. Personal data being obtained by deception or coercion is unfair and perhaps unlawful.

6.1.7 **DPP1(3) requires a data user to inform the data subject, on or before collection of his personal data, of the purpose for which the data are to be used, the classes of persons to whom the data may be transferred, and his rights to request access to and to request the correction of the data.**

6.1.8 It is a common practice for the data user to provide a written statement, generally referred to as a Personal Information Collection Statement (PICS), which should contain the purpose of use of the personal data and the classes of transferees of the data. A sufficiently clear, unambiguous and easy to understand PICS should be given to the data subject to take into account of the characteristics of the targeted data subjects (in terms of age, education level, etc.).

6.1.9 Many disputed cases between a data user and a data subject revolve around transfer of data to third party by the data user, e.g. transfer of data to an outsourced service provider for processing, or to a debt collection agency for debt recovery. A well drafted transfer clause will go a long way to minimise unpleasant surprise or dispute. Defining a class of transferees in vague terms such as “business partners” or “such third parties” should be avoided. A data user should define the class of data transferees by its distinctive features.

6.2 DPP2 - Accuracy and Duration of Retention of Personal Data

(1) All practicable steps shall be taken to ensure that-

(a) personal data are accurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used;

(b) where there are reasonable grounds for believing that personal data are inac curate having regard to the purpose (including any directly related purpose) for which the data are or are to be used-

(i) the data are not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or

(ii) the data are erased;

(c) where it is practicable in all the circumstances of the case to know that-

(i) personal data disclosed on or after the appointed day to a third party are materially inaccurate having regard to the pur pose (including any directly related purpose) for which the data are or are to be used by the third party, and

(ii) that data were inaccurate at the time of such disclosure, that the third party-

(A) is informed that the data are inaccurate; and

(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.

(2) Personal data shall not be kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data are or are to be used.

The Essence of DPP2

6.2.1 This provides that personal data should be **accurate, up-to-date and kept no longer than necessary.**

6.2.2 The meaning of "accurate" can be inferred from the definition of "inaccurate" under section 2(1), which, in relation to personal data, means the data is "incorrect, misleading, incomplete or obsolete".

6.2.3 It should be noted that the requirement for accuracy is not absolute, given the inevitability of human error. The duty of a data user under DPP2(1) is to take all reasonably practical steps to ensure the accuracy of all personal data held by it. For example, a bank would not breach DPP2(1) for holding an inaccurate correspondence address of a customer provided that it has taken prompt actions to verify the accuracy of the address and asked for update from the customer concerned.

6.2.4 According to DPP2(2), personal data held by a data user should be deleted when such data are no longer required for the purpose upon which they were collected. Moreover, section 26(1) of PD(P)O provides as follows:

"A data user shall erase personal data held by the data user where the data are no longer required for the purpose (including any directly related purpose) for which the data were used unless –

(a) any such erasure is prohibited under any law; or

(b) it is in the public interest (including historical interest) for the data not to be erased."

6.2.5 Generally, personal data will be kept for compliance with specific requirements provided by statues, codes of practice or guidelines applicable to a particular trade or industry. Some notable examples include:-

- In the cases where there are suspected money laundering activities, the banks are required to comply with the Guidelines on Prevention of Money Laundering issued by the Monetary Authority to combat money laundering and retain records for that purpose, with such records possibly containing personal data.

- The Inland Revenue Ordinance requires business records, and thereby personal data contained in them, to be kept for not less than 7 years.

- The Sex Discrimination Ordinance, the Family Status Discrimination Ordinance and the Disability Discrimination Ordinance allow for individuals to make a claim to a court of law against another for an act of discrimination. The Equal Opportunities Commission, which enforces these discrimination laws, allows relevant documents containing personal data to be kept for a defined period of time.

Guidance for Data Users for Compliance with DPP2

6.2.6 As the standard of accuracy varies according to circumstances, a greater degree of care should be taken to ensure accuracy where inaccuracy may entail serious consequences (the harm's test) as opposed to data concerning trivial or less serious matters.

- In application systems which hold and process personal data, there should be in place a sound sub-system of recording and updating of personal data to highlight data inconsistencies and optimise data accuracy, e.g. to include features of periodic triggering system to seek personal data updates from customers and employees, and where possible cross checking or referencing from different data sources for data validation.

- In application systems which hold and process personal data, there should be in place a sound sub-system of monitoring and triggering data deletion when necessary to comply with the requirements under DPP2(2) taking into account the requirements under statues, codes of practice and guidelines relevant to data retention and deletion.

6.3 DPP3 - Use of Personal Data

Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than-

(a) the purpose for which the data were to be used at the time of the collection of the data; or
(b) a purpose directly related to the purpose referred to in paragraph.

The Essence of DPP3

6.3.1 **In essence, in order not to contravene DPP3, the use of personal data must be for a purpose that is the same as or directly related to the purpose for which the data were to be used at the time of collection of the data by the data user. Otherwise, prescribed consent must be obtained from the data subject.**

6.3.2 The word "**use**" is defined in PD(P)O as including the **transfer and disclosure of data.**

6.3.3 DPP1(3) requires the data user to take practical steps to inform the data subject of the purpose of the use of his personal data prior to or at the time of data collection. This is usually achieved through the issue of a PICS. There is a general tendency for a data user in formulating PICS to frame the intended purposes in terms as general and wide as possible, couched in legalistic language and much fine prints, whereas the data subject usually has in mind specific use of his data for the intended purposes upon which his data were collected. Complaints and differing opinions on data use are usually due to differences in expectation between the data user and the data subject.

6.3.4 For example, for the opening of an account with a bank, the data subject would expect his personal data to be used for the relevant application processing, transaction servicing, billing and account maintenance. The data subject has a reasonable expectation that his data were to be used only for purposes directly related to his application for service, and sales and transfer of his data to a third party for a non-related purpose would likely be construed as a change of use inconsistent with the original purpose of data collection.

6.3.5 In many cases, the purposes of use of personal data cannot be exhaustively stated on or before the data collection by the data user. Therefore the concept of "directly related purpose" is of significance. A good example is the transfer of personal data, collected for the opening and maintenance of a credit card account, to a debt collection agency in case of default. This is considered as an activity directly related to the original purpose of data collection as the full and prompt settlement of all related debts outstanding is generally viewed as a legitimate component of the service rendered. However, the amount of personal data transferred to a third party, in this case a debt collector, should be adequate and necessary but not excessive in relation to debt recovery. In past cases investigated by PCPD, the Privacy Commissioner found that the transfer of a copy of the debtor's ID Card by a creditor to a debt collection agency was not necessary and was excessive for the purpose of debt recovery. Location and contact data would generally be sufficient.

6.3.6 Where the use of personal data is not the same as or directly related to the original purpose of collection, prescribed consent of the data subject has to be obtained. The meaning of the term "prescribed consent" is stated under Section 2(3) of PD(P)O as follows:

> "the prescribed consent of a person
> (a) means the express consent of the person given voluntarily;
> (b) does not include any consent which has been withdrawn by notice in writing served on the person to whom the consent had been given…."

6.3.7 It should be emphasised that the prescribed consent has to be **express**, meaning no such consent is to be implied from conduct of omission by the data subject; and the prescribed consent has to be given **voluntarily**. In ascertaining whether the consent is voluntarily given, the Privacy Commissioner would give due regard to such factors as whether the data subject is in fact free to choose between giving and withholding consent, without fear of any adverse consequence either way, whether there is deception or coercion, together with whether the consent is a so called "bundled consent" where the data subject has no real choice not to give. A typical example of "bundled consent" is where a customer is only provided with one space on an application form to sign and he has to choose between (i) giving up the application for the service and (ii) giving his "bundled consent" agreeing to the terms and conditions for the provision of the service originally sought as well as the use of his personal data prescribed by the data user when in fact he finds such prescribed use objectionable.

Guidance for Data Users for Compliance with DPP3

6.3.8 The use of personal data is defined to include transfer and disclosure. In order to comply with DPP3, the following considerations should be taken in deciding whether or not to transfer or disclose personal data:

- A data user should take into account the reasonable expectation of the data subject in the use of his personal data.
- The data user should examine the purpose of use of the personal data and the classes of transferees of the data as specified in PICS and see if the purpose of the intended transfer or disclosure of personal data is the same as or directly related to the original collection purpose that the intended recipient of the data falls within one of the classes of transferee.
- When in doubt and to avoid misunderstanding and unwanted consequences, it would be best to obtain prescribed consent from the data subject for the use of his personal data.
- In personal data transfer and disclosure to a third party, please ensure that such transfer is in line with the intended purpose of data use, and that the amount of data transfer should be adequate and necessary but not excessive in relation to fulfilling the purpose of the transfer.

6.4 DPP4 - Security of Personal Data

All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorised or accidental access, processing, erasure or other use having particular regard to-

(a) the kind of data and the harm that could result if any of those things should occur;
(b) the physical location where the data are stored;
(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;
(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
(e) any measures taken for ensuring the secure transmission of the data.

Guidance for Data Users for Compliance with DPP4

6.4.1 These recommendations are intended to assist in applying DPP4 during the development and setting up of an IT system and during its ongoing operation. These recommendations focus on practicable steps that can be taken to protect personal data against unauthorised or accidental access, processing, erasure or other use, but are not intended as an exhaustive set of information security protections.

General Guidance

6.4.2 There are several high-level forms of guidance that can be taken into consideration when developing a strategy for protecting personal data held in IT systems. These include:

Practicality

6.4.3 DPP4 requires "all practicable steps" to be taken to protect personal data. This does not call for an absolute assurance of protection, but rather that all practical and reasonable protection measures should be taken.

Type of Access

6.4.4 DPP4 addresses the risks to personal data from deliberate, unauthorised as well as accidental access, processing, erasure or other uses (including disclosure). The goal is the protection of personal data from all risks.

Degree of Harm

6.4.5 DPP4(a) provides that the selection and strength of protection mechanisms should be based on the degree of harm that would result from unauthorised as well as accidental access, processing or erasure of the personal data involved.

Physical Location

6.4.6 DPP4(b) says that the physical location of personal data is important from the perspective of understanding the threat environment and determining an appropriate level of protection.

System Security Measures

6.4.7 DPP4(c) suggests that security measures should be incorporated into any equipment in which the data are stored. Many of the practicable steps that can be taken to protect personal data are security features in the operating systems and system applications on which personal data is stored and processed, as well as the physical protections afforded to these systems.

User Integrity and Competence

6.4.8 Technological security mechanisms can provide the foundation for protecting personal data, but DPP4(d) advocates that they will only be effective when complimented by the integrity, prudence, and competence of the people with access to the data.

Secure Transmission

6.4.9 As bandwidth increases and computing models evolve, the location of personal data and the location of the people accessing it are increasingly not the same. Therefore, it is critical to ensure the protection of personal data transmission, including that which is not obvious to the end user, in order to satisfy DPP4(e).

Specific Guidance

6.4.10 This section contains specific guidance for technical measures and related procedural activities that can assist IT professionals in developing and maintaining systems that help to ensure the security of personal data. This is not an exhaustive checklist, but rather a series of practical recommendations for addressing common situations and issues.

6.4.11 These guidance are grouped into common themes. Each guidance contains additional information relating to the rationale or benefit of the recommendation.

Scoping

6.4.12 List each type of personal data that your system will contain.

- This list can come from a PIA. DPP4 applies to those systems, including computers, applications and network connectivity, that store or transmit personal data. By explicitly identifying the types of personal data that your system will contain, you will be able to ensure that your security measures address all the protection needs for each type of personal data in the relevant systems.

Storage of Personal Data

6.4.13 List each of the applications or locations in which personal data will be stored.

- These can include commercial applications such as DBMSs or ERP or CRM applications, file servers, or applications that are being custom developed for a specific business purpose. Compiling this list will help you ensure that all of the personal data on your systems is afforded the appropriate protection. It further assists you in knowing what security mechanisms, e.g. access control, are available for your use since the first line of protection for data comes from the applications managing the data.

6.4.14 Minimise the number of different applications and locations in which the personal data is stored.

- This reduces the scope of security work that needs to be done.

6.4.15 Optimise for sharing and working on personal data "in place," such as within an ERP or CRM application.

- This minimises the need to email personal data or to download it onto PCs, laptops, or USB drives, which again reduces the scope of security work, both in terms of the number of storage devices that need to be protected as well as the number of network communications channels that need to be protected.

Access Control

6.4.16 Define or create access control models so that it is easy to grant users access to the minimal amount of personal data they need to do their jobs.

- This can be accomplished through the use of Role Based Access Control (RBAC). By focusing on the information required by a job function instead of an individual, it is much easier to manage access control permissions in a dynamic user environment and to understand the minimum amount of information required by people to do their jobs.

6.4.17 For each type of personal data, designate an owner or a custodian who is responsible for deciding who may be granted access to these data.

- IT administrators have responsibility for implementing personal data policy decisions through the configuration of system access controls. However, the policy decisions themselves should be made by staff who are knowledgeable about the organisation's use of personal data and have been explicitly assigned responsibility for making these policy decisions. These are the personal data owners or custodians.

6.4.18 There should be a formal process, and associated electronic or paper forms, for requesting and approving access rights to personal data.

- The IT administrators who are responsible for configuring access should have an official list of the staff, i.e. data owners or custodians, who are authorised to grant access to personal data. This eliminates possible ambiguity in data access requests and makes it easier for administrators to do their jobs.

6.4.19 A user's access to personal data should be revoked when a change in job function means the user no longer needs that access to perform his duties. All access, as well as accounts, should be revoked when a user leaves the organisation.

- These are often overlooked activities that expose personal data to unnecessary risks of exposure.

6.4.20 There should be a periodic review of current access permissions to determine if they are up to date, based on individuals' work responsibilities.

- This provides a mechanism for helping to ensure that users have access to the minimum personal data they need to do their jobs, thus reducing risks of unauthorised use or exposure.

Audit

6.4.21 Create or use an auditing mechanism to track access to personal data.

- The types of personal data access to be audited should be configurable in order to balance system performance and accountability. The degree and type of auditing should be based on the sensitivity of the personal data and the impact of unauthorised access.

6.4.22 All administrator actions should be audited.

- The general lack of control over administrator actions, in particular access to data, presents a significant potential risk to personal data. Auditing is one way of mitigating this risk.

6.4.23 The audit mechanism should ensure the integrity of the audit records; in particular, it should prevent undetectable deletion or modification of audit records.

- An audit trail is only useful if the integrity of its contents can be guaranteed.

6.4.24 There should be tools that make it easy to review and process the audit trail.

- The volume of audit information can easily exceed the human capacity to review and analyse it. Automated tool is an important element in making sure that audit records relating to personal data access and use are reviewed in a timely manner.

6.4.25 The audit trail should be reviewed by someone who is not a user of the audited system.

- This avoids a potential conflict of interest as well as potential cover-up of inappropriate use of personal data.

Identification and Authentication

6.4.26 All users, including administrators, should use named accounts and not to share accounts.

- These measures are necessary in order to audit user actions. If there is an operational requirement to share administrator or operator accounts on a shift basis, then there should be formal documentation identifying who is using each account during each shift so that they can be held accountable for their actions.

6.4.27 The system should have password composition rules, including those for minimum length and complexity.

- To the greatest extent possible, the system should have features built in that make it easier for users to create strong passwords.

6.4.28 Passwords should be protected by message digests when stored so that neither hackers nor people with administrative privileges will be able to discover a user's password.

- Since message digests do not require the use of a secret encryption key, their use is less complex to develop than encryption. Further, their use eliminates many opportunities for accidental or deliberate compromise of passwords.

6.4.29 Passwords should always be encrypted when transmitted over networks.

- It is important that passwords are always encrypted and not just during the logon process. In particular, passwords should never be emailed in clear text.

6.4.30 Information about a user, such as his Hong Kong ID number, should never be used as a password.

- A Hong Kong ID card can be used to authenticate a person in person because of security features in the card itself. A Hong Kong ID number, by itself, can be used to identify a person; but cannot be used to authenticate him because Hong Kong ID numbers may be disclosed to third parties for different purposes, such as entering an office building. Organisations should not use any information about a person that can be collected by third parties when assigning passwords.

6.4.31 Users should change a new password immediately after it has been assigned.

- This minimises the risk that someone involved in the process of generating or transmitting the password to the user could use it themselves.

Encryption of Stored Data

6.4.32 Personal data on all portable devices should be encrypted.

- Portable devices include laptops, smart phones, music players, tablets, USB and removable disk drives, CDs, DVDs, etc. These devices have a high probability of being lost or stolen and so the risk to personal data residing on them is high. Both hardware and software solutions that provide automatic and mandatory encryption of data written to portable storage devices exist. These mitigate the risk of loss or theft in a way that does not place any additional burden on end users.

6.4.33 Personal data on PCs and servers should be encrypted if there is a risk of theft.

- This decision should be made in light of the physical protection of the offices or facilities in which the PCs or servers are located.

6.4.34 Backups should be encrypted.

- Reliance on physical protection of backup media is not sufficient. This is especially true when the storage and transportation of backup media is handled by a third party service provider or the backup media is transported offsite for storage.

Encryption of Transmitted Data

6.4.35 Effort should be expended to design a system so that the transmission of personal data is minimised or unnecessary.

- See the recommendations in the “Storage of Personal Data” section. A system design that minimises the transport of personal data and the number of protocols used for transport of personal data requires fewer protection mechanisms to secure and reduces the risk exposure to personal data.

6.4.36 All personal data transmitted across public networks, e.g. the Internet, should be encrypted.
- Encryption should be enabled by default for all of the network connections over which personal data may transit to protect it from interception by those with access to the intermediate network links and nodes.

6.4.37 Highly sensitive personal data whose unauthorised disclosure could cause grave harm should also be encrypted when transmitted over any network, including internal corporate networks.
- This protects against the intra-organisational threat of network sniffing.

6.4.38 Personal data should always be encrypted when transmitted over a wireless network.
- The WEP (Wired Equivalent Privacy) protocol has known vulnerabilities and so should not be used. The WPA2 (Wi-Fi Protected Access 2) protocol is a better alternative, though it is still important to choose strong encryption keys and rotate them regularly.

6.4.39 Email containing personal data should be protected via standards-based email encryption, such as S/MIME, or the use of encrypted attachments.
- In the case of encrypted attachments, passwords should be transmitted "out of band," e.g. over the phone, in person, or via SMS.

Security of Machines Holding Personal Data, Including PCs, Laptops and Smart Phones

6.4.40 Any computers that are used for work-related activities such as storing or processing personal data should be the property of the organisation and under its administrative control.
- Without these organisational and technical controls, security of any stored personal data cannot be assured.

6.4.41 Users should not have administrative rights on these machines, nor have the ability to install software.
- Without these technical measures many security controls cannot be enforced.

6.4.42 Procedures should be in place for the prompt installation of security patches and updates.
- Many virus and other malware infections take place after security patches have been developed, but not yet installed. Prompt installation reduces this window of vulnerability.

6.4.43 Anti-malware software should be installed and configured to automatically install new malware signatures.
- This also reduces the window of vulnerability to malware infection.

6.4.44 The organisation should define the set of authorised software that can be installed on these machines and periodically verify that unauthorised software is not present.
- File sharing and P2P applications are particularly dangerous and should not be permitted unless there is a compelling business requirement for them.

6.4.45 A firewall should be installed on a computer if it may be used in an environment in which it is not protected by a corporate firewall.
- The firewall should have the functionality to detect and notify users of outgoing connections that could be used by malware for surreptitiously extracting personal data.

6.4.46 All computers should be configured to require a username and password (or some other forms of authenticators) for login.
- This will prevent unauthorised access to personal data when users are away from their computers.

6.4.47 Password-protected screen savers should be used.
- This will prevent unauthorised access to personal data when users are away from their computers.

6.4.48 Smart phones should be protected by a password or PIN, and the contents should be encrypted, if possible.
- This helps protect personal data in the event a smart phone is lost or stolen.

6.4.49 Remote administration software should be strictly controlled and require a user explicitly authorise remote access.
- When improperly configured or used, remote administration software can be used as an attack vector, resulting in unauthorised access to personal data.

6.4.50 Where supported, remote erasure and locking of smart phones should be enabled in the event of loss or theft.
- Note that the erasure and locking should be done before instructing the mobile service provider to discontinue service.

Server Security

6.4.51 Servers should be located in a locked server room or data centre and access should be limited to those administrators and operators with responsibility for maintaining the servers.
- This reduces the risk of unauthorised access to personal data, as well as potential damage to systems containing personal data, from someone with physical access to the console.

6.4.52 Procedures should be in place for the prompt installation of security patches and updates.
- Many virus and other malware infections take place after security patches have been developed, but not yet installed. Prompt installation reduces this window of vulnerability.

6.4.53 Anti-malware software should be installed and configured to automatically install new malware signatures.
- This also reduces the window of vulnerability to malware infection.

6.4.54 Servers should be protected by a corporate firewall.
- This is an important element of a security strategy to protect against external attack.

6.4.55 Administrator passwords should be changed whenever an administrator leaves the organisation.

- This is critical given the virtually unlimited access to information, including personal data, that administrator passwords enable.

6.4.56 Logs and audit trails for servers and other core infrastructure, such as firewalls and routers, should be periodically reviewed for anomalies and possible attacks.

- The frequency and degree of analysis to which logs and audit trails are reviewed should be based on the degree of consequence of unauthorised disclosure of the personal data and the threat environment in which the systems are operating.

6.4.57 All servers, devices and network connections should be clearly labelled and network connections that are not in use should be disconnected.

- Over time, IT systems are replaced, augmented and their use evolves. Strong configuration controls can help prevent unauthorised access to systems containing personal data.

Recycling of Computing Devices

6.4.58 Computers that are being reassigned within an organisation should undergo the following steps:

1. The disk should be defragmented.
2. The disk should be reformatted.
3. The operating system and applications should be reinstalled.
4. Unallocated space should be securely erased.
    - These measures will prevent the new user of a computer from being able to gain access to any of the personal data that was previously stored on the computer.

6.4.59 The memory of all computing devices, including smart phones, should be securely wiped before the devices leave the organisation.

- This will prevent anyone, including someone with computer forensic tools, from being able to gain access to any of the personal data that was previously stored on the computer.

Hard Copy

6.4.60 Printing of personal data should be minimised as much as possible.

- This reduces the opportunity for hard copy of personal data to be lost or stolen, as well as reduces the task of properly disposing of personal data.

6.4.61 Any printers that could be used for printing personal data should be in a physically controlled environment in which only people who are authorised for access to personal data have unescorted or unsupervised access.

- This addresses the risk of hard copy of personal data being removed from a printer before the person who printed it has the chance to pick it up.

6.4.62 Highly sensitive personal data should only be printed on printers in tightly controlled environments, for example in a staff member's personal office.

- This typically addresses situations in which there is a low volume of printing, but the consequences of loss or disclosure of the personal data is high.

6.4.63 Printers or photocopiers that support secure printing, where passcode can be assigned to each print job and the printout would not be printed until the correct code is entered at the printers/ photocopiers, should be promoted for printing for use where personal data is to be printed.

- This reduces the need to purchase printers for each staff members who may have occasional needs to print personal data.

6.4.64 Printers or photocopiers that contain internal hard drives should be physically protected and should utilise available security features to prevent access to the data on the hard drives. These features can include access controls on the drives, encrypting the drives, and securely erasing data after it has been printed, copied, scanned or faxed. When it comes to the disposal of printers or photocopier, any internal hard drives should be securely disposed of too.

- This ensures that personal data stored in the printers or photocopiers will not be accessed or used by unauthorised persons.

6.4.65 Hard copy of personal data should be stored in a locked container, e.g. file cabinet or desk drawer, when not in use.

- Promulgation of a clean desk policy may assist in ensuring that hard copy of personal data has the appropriate physical protection.

6.4.66 Hard copy of personal data should be properly destroyed, for example by a cross cut shredder, when no longer needed.

- The method used for destruction of hard copy of personal data should be convenient for staff to use.

Organisational Issues

6.4.67 All staff with access to personal data should have job-specific training and education on their responsibilities for protecting personal data.

- For example, end users may need training on choosing strong passwords or using email encryptions. Administrators, on the other hand, may need training on guidelines for audit trail review. All staff should receive training in their responsibilities vis-á-vis protecting and using personal data.

6.4.68 Any third party to whom personal data is entrusted needs to support sufficient IT security mechanisms and associated procedures.

- The recommendations outlined here can be used by third party service providers as part of their strategy for protecting personal data. Depending on the nature of the services provided and their own business operations, these service providers may also need to provide additional assurance or explanation of how they enforce separation between personal data provided by one organisation and information belonging to other organisations.

6.5 DPP5 - Information to Be Generally Available

All practicable steps shall be taken to ensure that a person can-

(a) ascertain a data user's policies and practices in relation to personal data;
(b) be informed of the kind of personal data held by a data user;
(c) be informed of the main purposes for which personal data held by a data user are or are to be used.

The Essence of DPP5

6.5.1 This provides for openness by data users about the kinds of personal data they hold and the main purposes for which personal data are used.

6.5.2 DPP5 requires a data user to take reasonably practicable steps to **make known and be transparent about its policy and procedures** that apply to its collection, retention and use of personal data.

Guidance for Data Users for Compliance with DPP5

6.5.3 A data user should have a written policy statement, commonly referred as a Privacy Policy Statement (PPS) which states the kind of personal data it held, and the various purposes for which personal data are being used or to be used. Other relevant information, such as the data retention periods and the right of data subjects to access and correct their personal data, would be relevant for reasons of transparency and clarity to gain customers' and employee's confidence.

6.5.4 The PPS should be regularly reviewed in line with changing business requirements and regulatory demands which have impacts upon the use of personal data collected and held.

6.5.5 The availability and contents of the PPS should be effectively communicated to the data subjects when and where their personal data are being collected or to be collected, e.g. public and noticeable display of PPS where CCTV is used for security reasons, home page of Internet websites which collect and display personal data, or verbal or recorded communications of PPS contents during telephone interaction with their customers at call centres.

6.5.6 Due to the perceived and highly privacy intrusive nature of workplace monitoring of staff, the availability, clarity and comprehensiveness of PPS and its effective communications to employees are of significant importance.

6.6 DPP6 - Access to Personal Data

A data subject shall be entitled to-

(a) ascertain whether a data user holds personal data of which he is the data subject;
(b) request access to personal data-
  (i) within a reasonable time;
  (ii) at a fee, if any, that is not excessive;
  (iii) in a reasonable manner and
  (iv) in a form that is intelligible;
(c) be given reasons if a request referred to in paragraph (b) is refused;
(d) object to a refusal referred to in paragraph (c);
(e) request the correction of personal data;
(f) be given reasons if a request referred to in paragraph (e) is refused, and
(g) object to a refusal referred to in paragraph (f).

The Essence of DPP6

6.6.1 This provides for data subjects to have rights of access to and correction of their personal data. PD(P)O also contains other provisions upon which such access and correction could be refused.

Right of Data Access

6.6.2 DPP6, together with Section 18(1) of PD(P)O, provides an individual with the right:
a. to be informed by a data user whether the data user holds personal data of which he is the data subject;
b. if the data user holds such data, to be supplied by the data user with a copy of such data.

6.6.3 To avoid confusion, misunderstanding and possible oversight on the part of the data user that an incoming communication is an access request under PD(P)O, the Privacy Commissioner, pursuant to his power to specify form[1] under PD(P)O, has specified a Data Access Request Form in which data access requests are to be made. This prescribed form can be found in http://www.pcpd.org.hk. A data user **may** refuse a data access request which is not made in this prescribed form[2].

[1] Section 67(1) of PD(P)O
[2] Section 20(3)(e) of PD(P)O

6.6.4 Unless there are legitimate grounds for refusal, (see paragraphs 6.6.6 to 6.6.8 below), a data user shall comply with a data access request **not later than 40 days after receiving the access request**[1]. A data user who refuses to comply with a data access request shall send a notice of refusal with reasons to the requestor not later than 40 days after receiving the request[2], and a data user who fails to comply with a data access request within 40 days shall inform the requestor with explanation in writing and subsequently comply with the request as soon as practicable after the expiration of the 40 days[3].

6.6.5 A data user can impose a fee for complying with a data access request[4]. However, the fee **should not be excessive**. The meaning of not being excessive should be construed[5] as confining the fee only to cover those costs which are directly related to and necessary for complying with a data access request. Generally speaking, the data user bears the evidentiary burden to show that the fee it imposes does not exceed its direct and necessary costs.

6.6.6 A data user shall **refuse to comply with a data access request** if the data user is not supplied with such information as the data user might reasonably require in order to establish the identity of the requestor[6]. Without the appropriate identification of the requestor, a data user might inadvertently or erroneously disclose personal data of a data subject to another individual, an act which could be in breach of DPP3, i.e. the disclosure is made to a third party not in line with the purpose for which the data should be used.

6.6.7 A data user shall **also refuse to comply with a data access request** if the data user cannot comply with the request without disclosing personal data of which another individual is the data subject[7], unless the data user is satisfied that the other individual has consented to the disclosure of his data to the requestor. However, where there is no such consent, the data user may comply with the request by erasing from the data the name and other explicit identification of the other individual before releasing a copy of the data to the requestor.

6.6.8 The foregoing paragraphs deal with the situations where a data user must refuse to comply with the data access requests. The following provides other grounds where a data user **may refuse to comply with a data access request**:-

(a) if the request is not in writing in the Chinese or English language[8];

(b) if the data user is not supplied with such information as the data user may reasonably require to locate the personal data to which the request relates[9];

[1] Section 19(1) of PD(P)O
[2] Section 21(1) of PD(P)O
[3] Section 19(2) of PD(P)O
[4] Section 28 of PD(P)O
[5] AAB No. 37/2009
[6] Section 20(1)(a) of PD(P)O
[7] Section 20(1)(b) of PD(P)O
[8] Section 20(3)(a) of PD(P)O
[9] Section 20(3)(b) of PD(P)O

(c) if the request follows 2 or more similar requests and it is unreasonable in all the circumstances for the data user to comply with the request[1];
(d) any other data user controls the use of the data in such a way as to prohibit the first-mentioned data user from complying (whether in whole or in part) with the request[2];
(e) unless and until any fee imposed by the data user for complying with the request has been paid[3];
(f) if the request is not made in the prescribed form specified by the Privacy Commissioner[4];
(g) compliance with the request may for the time being be refused under PD(P)O, whether by virtue of an exemption[5] or otherwise[6].

6.6.9 **The notice of a refusal** by the data user to comply with the data access request shall be made to the **requestor not later than 40 days after receiving the request** and a log book with entries of refusal should be kept and maintained by the data user. The particulars in the log book must be kept for a minimum period of four years.

Right of Data Correction

6.6.10 The term "**correction**", in relation to personal data, means *"rectification, erasure or completion"*[7].

6.6.11 Having been supplied by a data user with a copy of his personal data in compliance with an earlier data access request, an individual has the right to make a data correction request if he considers that the personal data provided are inaccurate[8]. It therefore follows that a data correction request must be preceded by a data access request.

6.6.12 A data user who is satisfied that personal data to which a data correction request relates are inaccurate, shall, not later than 40 days after receiving the request:
(a) make the necessary correction to those data;
(b) supply the requestor with a copy of those data as so corrected; and
(c) if those data have been disclosed to a third party during the 12 months immediately preceding the day on which the correction is made, take all practicable steps to supply the third party with a copy of data so corrected and accompanied by a notice in writing stating the reasons for the correction[9].

[1] Section 20(3)(c) of PD(P)O
[2] Section 20(3)(d) of PD(P)O, but this ground of refusal does not apply to a data access request made under section 18(1)(a); or where the request is made under section 18(1)(b), to any extent that the data user can comply with the request without contravening the prohibition concerned
[3] Section 28(5) of PD(P)O
[4] Section 20(3)(e) of PD(P)O
[5] Part VIII of PD(P)O
[6] Section 20(3)(f) of PD(P)O
[7] Section 2(1) of PD(P)O
[8] Section 22(1) of PD(P)O
[9] Section 23(1) of PD(P)O

6.6.13 Unlike a data access request, a data user cannot impose any fee for compliance with a data correction request.

6.6.14 Similar as in the case of a data access request, a data user **shall refuse to comply with a data correction request** if the data user is not supplied with such information as the data user might reasonably require in order to establish the identity of the requestor[1].

6.6.15 A data user **may refuse to comply with a data correction request** if:
(a) the request is not in writing in the Chinese or English language[2];
(b) the data user is not satisfied that the personal data to which the request relates are inaccurate[3];
(c) the data user is not supplied with such information as the data user may reasonably require to ascertain in what way the personal data to which the request relates are inaccurate[4];
(d) the data user is not satisfied that the correction which is the subject of the request is accurate[5];
(e) any other data user controls the processing of the personal data to which the request relates in such a way as to prohibit the first-mentioned data user from complying (whether in whole or in part) with the request[6].

6.6.16 Where a data user refuses to comply with a data correction request, the following steps should be taken:
1. enter into a log book the particulars of the reasons for the refusal[7]. The particulars in the log book must be kept for a minimum period of four years; and
2. inform the requestor in writing of the refusal and the reasons of the refusal not later than 40 days after receiving the request[8].

Guidance for Data Users for Compliance with DPP6

6.6.17 For IT applications which collect and process personal data, there should be a log subsystem to handle data access and correction requests, which should include such features as:

- Log the date when a data access/correction request is received and monitor related actions of compliance or refusal within the subsequent 40 days;
- Trigger the necessary response to the requestor in good time before the expiry of the 40-day period; and
- Create and maintain a log book on refusals to data access and correction requests and reasons for such refusals.

[1] Section 24(1)(a) of PD(P)O
[2] Section 24(3)(a) of PD(P)O
[3] Section 24(3)(b) of PD(P)O
[4] Section 24(3)(c) of PD(P)O
[5] Section 24(3)(d) of PD(P)O
[6] Section 24(3)(e) of PD(P)O, but this ground of refusal does not apply to the data correction request concerned to the extent that the data user can comply with the request without contravening the prohibition concerned
[7] Section 27(2)(c) of PD(P)O
[8] Section 25(1) of PD(P)O

6.7 Exemptions

What are Exemptions?

6.7.1 Privacy, including personal data privacy, is a fundamental human right, and PD(P)O aims to protect the individual's right to personal data privacy in Hong Kong. However, individual's human rights are not absolute, as they should be considered together with the overall rights of a society, in other words, the overall public interests of a society.

6.7.2 While PD(P)O generally requires the compliance with the six DPPs and other provisions in personal data handling by data users, there are exceptional circumstances when the overall public interests are taken into consideration. These exceptions are commonly referred to as exemptions.

6.7.3 Generally speaking, most exemptions apply to DPP3 which governs the use of personal data, and DPP6 which provides the right of data access. For illustrative purpose, let us consider the situation where a law enforcement agency approaches a bank for account information relating to an account holder who is suspected of carrying out money laundering activities. The personal data of the account holder was collected and used by the bank for the purpose of administrating the bank account, and should not be used (where "use" includes transfer and disclosure) for any other non-related purpose. The exemption which applies to the prevention and detection of crime would allow the bank as a data user to consider and where relevant disclose to the law enforcement agency the account information data. In other words, a change of use for a different purpose takes place without the prescribed consent of the account holder, which is a breach of DPP3 in normal circumstances if not for this exemption.

6.7.4 Using the same example, the account holder, suspicious of probes by law enforcement or merely fishing for information, submits a data access request to the bank to obtain a copy of his personal data and its use. With the exemption of crime detection and prevention, the bank would not be obliged to reveal that his account data have been disclosed to the law enforcement agency.

6.7.5 All the exemption provisions can be found in Part VIII of PD(P)O. The following is a partial list which has the widest scope or is commonly encountered:

6.7.6 **Section 52 Domestic Purposes**

"Personal data held by an individual and –

(a) concerned only with the management of his personal, family or household affairs; or
(b) so held only for recreational purposes,

are exempt from the provisions of the data protection principles, Parts IV and V and sections 36 and 38(b)."

6.7.7 This is a very broad exemption provision. It covers personal data held for domestic or recreational purposes, e.g. telephone and address lists of personal friends, guest lists for Christmas party or family wedding.

6.7.8 **Section 58 Detection and Prevention of Crime etc**

This section probably has the widest application, and thus deserves to be listed here.

Personal data held for the following purposes:

"(1) (a) the prevention or detection of crime;
(b) the apprehension, prosecution or detention of offenders;
(c) the assessment or collection of any tax or duty;
(d) the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;
(e) the prevention or preclusion of significant financial loss arising from –
(i) any imprudent business practices or activities of persons; or
(ii) unlawful or seriously improper conduct, or dishonesty or malpractice, by persons"

are exempted from the provisions of data protection principle 6 and section 18(1)(b) where the application of those provisions to the data would be likely to –

(i) prejudice any of the matters referred to in this subsection; or
(ii) directly or indirectly identify the person who is the source of the data.

(2) Personal data are exempt from the provisions of data protection principle 3 in any case in which -
(a) the use of the data is for any of the purposes referred to in subsection (1) (and whether or not the data are held for any of those purposes); and
(b) the application of those provisions in relation to such use would be likely to prejudice any of the matters referred to in that subsection."

6.7.9 **Section 59 Health Data**

Section 59 exempts physical and mental health data from the provisions of DPP3 and DPP6 when:

". . . the application of those provisions to the data would be likely to cause serious harm to the physical or mental health of –

(i) the data subject; or
(ii) any other individual."

6.7.10 Health data of an individual are always regarded as confidential and sensitive and usually not to be disclosed. However, under certain circumstances when the potential harm of non-disclosure outweighs the right of data privacy, this exemption would come into play. An example is the disclosure by a medical doctor to his patient's spouse or sex partner when the patient is found to have a serious transmittable disease, e.g. AIDS.

6.7.11 **Section 62 Statistics and Research**

Section 62 concerns the use of personal data for preparing statistics or carrying out research. It exempts personal data from the application of DPP3 when the following conditions are satisfied:

"(a) the data are to be used for preparing statistics or carrying out research;
(b) the data are not to be used for any other purpose; and
(c) the resulting statistics or results of the research are not made available in a form which identifies the data subjects or any of them."

6.7.12 The particular requirement to note is that the resulting statistics or research does not reveal the identities of the data subjects, or is not compiled in such a way that makes it reasonably practicable for their identities to be ascertained.

6.8 Checklist for Data Users in Ensuring Compliance with PD(P)O

6.8.1 The following are the pertinent questions that a data user should properly address in order to ensure that its personal data management practice complies with the requirements under PD(P)O:

1. Is there any function or activity involving the collection of personal data? Is the collection of personal data directly related to the function or activity?

2. What are the purposes of use? Is collection of personal data necessary for or directly related to the purposes? Are the means of collection lawful and fair? Are data collected adequate but not excessive in relation to the purpose?

3. What information should be provided to the data subject on or before collection? (Please refer to Section 6.1 for the requirements under **DPP1**.)

4. What are the practicable steps taken to ensure data accuracy and how long will the collected personal data be retained before erasure? (Please refer to Section 6.2 for the requirements under **DPP2** and **section 26**.)

5. Does the use (which includes disclosure and transfer) of personal data fall within the original purpose of collection or its directly related purpose? (Please refer to Section 6.3 for the requirements under **DPP3** and Section 6.7 for the appli cability of the exemption provisions.)

6. What are the practicable steps taken to ensure that there are in place adequate security measures so that personal data collected are protected from unauthorised or accidental access, erasure or other uses? (Please refer to Section 6.4 for the requirements under **DPP4**.)

7. Are there privacy policies and practices in place and made generally available? (Please refer to Section 6.5 for the requirements under **DPP5**.)

8. Are the data access requests and data correction requests received being properly handled? (Please refer to Section 6.6 for the requirements under **DPP6**.)

9. Are there any applicable exemptions from compliance with the relevant requirements under PD(P)O? (Please refer to Section 6.7 for the exemption provisions under **Part VIII** of PD(P)O.)

Chapter 7
Practical Guidelines on Major Topics Related to IT and Technology Applications

7.1 Outsourcing and Cloud Computing

Introduction

7.1.1 Due to limited resources, many organisations have turned to IT outsourcing as one of their key organisational strategies in order to face the challenge of meeting the ever-increasing demands of customers and the marketplace. IT outsourcing can cover a range of different services including application development and maintenance, network management, desktop management, IT helpdesk services, computer data centre management and subscription of cloud computing services. Such outsourcing work would usually involve the transfer from the organisations of substantial amount of data, including personal data, to the outsourcing agent for storage, access and processing.

7.1.2 Under PD(P)O, an outsourcing agent is not taken to be a data user if he holds, processes or uses personal data solely on behalf of another person, and not for his own purposes1. Not being a data user, the outsourcing agent is not required to comply with the requirements under PD(P)O including DPPs. A data user who engages an agent for data processing, however, shall be held liable for acts of non-compliance of PD(P)O done by his agent in handling or processing personal data in the course of the outsourcing.

Guidance

7.1.3 In discharging his responsibility and liability, it is paramount for a data user to ensure the handling of personal data transferred to and processed by his outsourcing agent are in compliance with PD(P)O and its DPPs. Towards this objective, the following recommendations are relevant:

- In the selection process of an outsourcing agent, the agent should demonstrate an adequate understanding of the requirements under PD(P)O in handling personal data, and has developed an organisational culture of respecting personal data privacy through practice, education and training. For guidance in strategy and policy for personal data protection at the enterprise level, please refer to Chapter 3.
- For outsourcing which involves the transfer to and processing of personal data by the outsourcing agent, a Privacy Impact Assessment (PIA) should be conducted on the outsourcing activity to evaluate its potential impact upon personal data privacy with the objective of avoiding or minimising adverse effect. For further details of PIA please refer to Chapter 3.
- Based on the requirements under PD(P)O and the findings of the PIA where appropriate, the contract with the outsourcing agent should include provisions which ensure adequate protection of personal data transferred to the agent by the data user as stipulated by PD(P)O, or equivalent protection if the agent is based overseas or the processing is conducted in overseas locations. In particular, personal data should only be used for the purpose of the outsourcing task and no other, and that the data would be adequately kept secure to protect against unauthorised or accidental access or use. Furthermore, the contract should stipulate the requirements regarding retention arrangement and deletion or return of personal data after satisfying the purpose for which the data were transferred to the agent.

- The outsourcing contract should also stipulate either the need for the agent to conduct regular audits or assessments to ensure adequate protection measures are in place, or allow the data user to conduct such regular audits or assessments.
- The data user and the outsourcing agent should follow the practical guidelines on the application of the six DPPs in systems design, development and operations in Chapter 6, in particular,
  - — DPP1 with respect to the purpose and manner of personal data collection
  - — DPP2 with respect to the accuracy and retention of personal data transferred to the outsourcing agent.
  - — DPP3 with respect to the proper and legitimate use of personal data by the agent
  - — DPP4 with respect to the security of the personal data transferred to and held by the agent.
- Very often, outsourcing involves the transfer to and use of personal data by an outsourcing agent for direct marketing purposes. Section 7.3 on direct marketing provides constructive guidance to both the outsourcing organisation as well as the agent in terms of the proper handling of personal data in direct marketing campaigns and operations.

Cloud Computing

7.1.4 In the past, the data flow the Internet world allows is from point-A-to-point-B, with the intermediary network being passive except for data routing. Processing or other utilisation of data was done at the communication's end points. Ensuring the privacy and security of data in such a transaction required three principal measures:

- appropriate security protections (e.g. firewalls) at the end-point servers,
- appropriate data collection and handling procedures at both points A and B, and
- security protection (encryption, generally) for data in motion.

7.1.5 However, the emergence of Cloud computing, particularly when utilising a public or hybrid Cloud architecture, forces clients to re-think the data protection schemes developed because the Cloud service providers become the new actor who is progressively being assigned more and more of the functions which formerly occurred within the internal servers and networks.

7.1.6 Securing information that enters the Cloud, and protecting the privacy associated therewith, thus requires a shift, moving protections deeper into the Cloud's infrastructure. As privacy issues are central to users' concerns about the adoption of Cloud computing, building such protections into the design and operation of the Cloud is vital to the future success of this new networking paradigm.

Guidance

7.1.7 A set of best practices for the development of a privacy-respecting Cloud computing architecture can be found in the Privacy by Design Principles, as developed by Dr. Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada. Based on the Privacy by Design Principles, privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organisation's default mode of operation. The Principles of Privacy by Design may be applied to all types of personal information, and may be accomplished by practicing the seven Foundational Principles. These Principles are fully treated in the document:

http://www.privacybydesign.ca/content/uploads/2010/07/pbd-NEC-cloud.pdf

7.1.8 A brief description of the seven Foundational Principles are as follows:

Proactive not Reactive; Preventative not Remedial

- The *Privacy by Design* approach is characterised by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. *Privacy by Design* does not wait for privacy risks to materialise, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to prevent them from occurring. In short, *Privacy by Design* comes before-the-fact, not after. Encryption is at the heart of the architecture, along with systems to ensure appropriate access to data is not reduced – maintaining the positive-sum paradigm.

Privacy as the Default

- It should not be assumed that a user has either the capability or capacity to oversee and control access rights to the entirety of his or her data. Thus, privacy must be protected by default. *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, his privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, *by default*.

Privacy Embedded into Design

- Privacy considerations must be taken into account during the design phase of a technology. *Privacy by Design* is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

Full Functionality – Positive-Sum, not Zero-Sum

- *Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretence of false dichotomies, such as privacy vs. security, demonstrating that it *is* possible to have both. Creating a privacy-protective Cloud architecture is, of course, meaningless if it is not also functional. The privacy of data should be assured, but so should appropriate access. The integrity of stored data should also be assured. A zero-sum approach forces trade-offs for the user, as well, who must determine which factors they value above others (privacy, security, functionality, etc.). For a paradigm shift as large as Cloud computing, the positive-sum must be realised in order to meet the technology's full potential.

End-to-End Security – Lifecycle Protection

- *Privacy by Design*, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.

Visibility and Transparency

- *Privacy by Design* seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike.

Respect for User Privacy

- Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric. Respect for user privacy is the overarching theme of *Privacy by Design*. Privacy should not be a box-checking exercise; it should instead be integrated into an organisation's culture. The reason for ensuring privacy – respect for the user – should be kept in awareness when designing systems. This may be seen in appropriate defaults, data minimisation, strong security measures, or the ability for the user to exercise control over his or her own data.

Useful References

Information and Privacy Commissioner, Ontario, Canada (Revised: January 2011), *Privacy by Design – The 7 Foundational Principles*
(http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf)

Information and Privacy Commissioner, Ontario, Canada (May 2010), *Modelling Cloud Computing Architecture Without Compromising Privacy: A Privacy by Design Approach*
(http://www.privacybydesign.ca/content/uploads/2010/07/pbd-NEC-cloud.pdf)

7.2 Workplace Monitoring

Introduction

7.2.1 Workplace monitoring, or employee monitoring, is now widely deployed across organisations for a variety of purposes, mainly to protect organisational interests. Such monitoring includes:

- **managing workplace productivity** such that employees' time and efforts are devoted during office hours to relevant organisational interests and not to personal or private purposes,

- **managing service quality**, e.g. through the recording of telephone conversations between employees and customers to ensure quality and consistency of customer service,

- **protecting a wide range of security requirements**, including premise security using closed circuit TV (CCTV) monitoring, or protection of leakage of business secrets through email monitoring,

- **compliance with statutory or regulatory requirements**, e.g. creating a video record of employees entrusted with the handling of hazardous materials to ensure adherence to safety and health regulations in the workplace.

7.2.2 The workplace monitoring applications commonly deployed include the following:

Email Monitoring
- Monitoring and recording employees' use of E-mail sent and received on equipment made available to them by the employer.

Telephone Monitoring
- Monitoring and recording telephone calls and voice mails made or received by employees on telecommunications equipment, including mobile phones, made available by the employer.

CCTV Monitoring
- Monitoring and recording employees' work activities and behaviours by the use of video recording or CCTV, or similar equipment.

Internet Monitoring
- Monitoring and recording employees' web browsing activities using equipment made available to them by the employer.

7.2.3 Where, and usually, workplace monitoring involves the collection of personal data, compliance with PD(P)O and adherence to its six DPPs (please refer to Chapter 6) are required. The optimum objective is to be able to balance the legitimate interests of employer and the personal data privacy interest of employees.

General Guidance

7.2.4 The introduction, implementation and operations of workplace monitoring applications should be accompanied by the following considerations:

- Assess the appropriateness and necessity of workplace monitoring (Why is monitoring necessary?);
  - Examples of concerns:-
    - Employee or Customer Safety
    - Confidentiality and Trade Secret Concerns
    - Workplace Liability and Investigations
    - Network and Systems Performance
    - Employee Productivity

- Assess its impact on the personal data privacy of employees

  - the kind of personal data to be collected
  - the sensitive nature of the data to be collected for the appropriate level of security to be assigned for its protection
  - the amount of data to be collected and kept to the minimum required to fulfil the purpose of monitoring

- Consider the use of less privacy intrusive alternatives to workplace monitoring where possible (Is this the only way?);
  - Examples:
    - For the purpose of compiling statistics on outbound telemarketing calls, a log from the telephone system is sufficient and hence could be used instead of telephone recording;
    - For the purpose of network capacity planning, the aggregate of network statistics by segments is sufficient and hence the detailed traffic pattern for individual employee is not necessary.

- Consult with employees in determining the parameters for a reasonable expectation of privacy at work (When and where the monitoring is to take place?);
  - Examples:
    - CCTV should be positioned in a way that will not unnecessarily intrude the privacy of individuals;
    - CCTV should not be placed in places where people have a reason to expect privacy (e.g. changing room, toilet);
    - Generally workplace monitoring should be conducted in an overt manner. Covert monitoring should not be adopted unless justified by special circumstances, e.g. absolutely necessary to collect evidence of an unlawful activity;
    - Time and duration of monitoring should be discussed with the employees.

- Implement a comprehensive Employee Monitoring Policy;
  - Content to be included:
    - The business purpose(s) that workplace monitoring seeks to fulfil;
    - The circumstances under which monitoring may take place and the manner in which monitoring may be conducted;
    - The kinds of personal data that may be collected in the course of monitoring;
    - The purpose(s) for which the personal data collected in monitoring records may be used;
    - Who may have access to the personal data collected and under what circumstance;
    - Retention period of recorded information.

- Communicate the Employee Monitoring Policy to employees;
  - The Employee Monitoring Policy allows both parties (employer and employee) to have a clear understanding on Why (the purpose), What (the areas such as email, internet, telephone, workplace), When (monitoring time and duration) and How (way in which the data would be collected and the treatment of the data thereafter) the monitoring would be conducted.

- Make known the areas and information being or to be captured by the monitoring applications;
  - Examples:
    - Wherever CCTV is in operation, a legible sign is posted to alert the personnel accessing the monitored areas;
    - If web content/email filtering software is in use to filter inappropriate contents under company policy, clear warning should be given to users.

- Implement appropriate security and access control measures to safeguard the security of personal data collected and stored in monitoring records against unauthorised and accidental access or erasure, or wrongful use. Please also refer to the section on DPP4 and data security in Chapter 6.

- Specify the retention period of personal data in the monitoring records;

  - Such data should not be kept longer than is necessary for the stipulated purpose for its collection. Generally speaking, retention period should not be longer than six months, though there are exceptions, e.g. as evidence for legal or contractual obligations.

- Provide appropriate training related to the workplace monitoring applications, and their requirements for security, privacy and PD(P)O to those personnel responsible for managing and operating such applications.

Specific Guidance

7.2.5 The following provides specific guidance for each type of monitoring activities:

Email Monitoring

Guidelines:

• IT administrator should only manage the communication logs for the purpose of proper email system functioning without a need to resort to examining the content of the email;

• IT administrator, if required, installs automatic tools for the purpose of system/security control (e.g. virus/spam) that needs to examine the content of the email digitally without revealing the content;

• Where appropriate, notice should be inserted to messages so that the senders and recipients are aware of the email monitoring action;

• Ensure there is a policy on how and when email communication records can be read by the employer.

Telephone Monitoring

Guidelines:

• In general, call monitoring or recording are necessary only under special business areas such as call centre;

• Though not mandatory, it is a good practice to inform the caller that the conversation is being recorded and the purpose of such recording;

• Where personal information is collected during the recording process, the collected information should be deleted when the purpose for such data collection no longer exists;

• Where personal information is collected during the recording process, reasonable security measures (please refer to the Guidance Section on DPP4 security in Chapter 6) must be in place to safeguard the information from unauthorised access and disclosure;

• Ensure there is a policy on how and when telephone conversation recording can be listened to by the employer;

• Ensure there is a data access request mechanism in place for customers as well as employees to request access to recording.

CCTV Monitoring

Guidelines:

• If such monitoring and recording is deemed necessary after evaluation, the CCTV should be installed in designated areas for effective monitoring to fulfil the purpose of such monitoring;

• A clear notice should be displayed so that people are aware that such monitoring is in operation;

• The personnel operating the CCTV should be trained and made aware of the proper procedure in handling the recorded data;

• The recorded image should be deleted as soon as practicable once the purpose of collection is fulfilled;

• Adequate measures should be in place (please refer to the Guidance Section on DPP4 security in Chapter 6) to safeguard the recorded image from unauthorised access and retrieval;
• Recording of conversation should not be carried out at the same time unless all parties concerned are well informed or in limited circumstances, such as at two-way audio "help points" that are covered by CCTV systems and the audio is activated by the person requesting assistance.

Internet Monitoring

Guidelines:
• Preventive approach by blocking inappropriate sites is better than detective approach where all clicks are recorded as the latter may enable capturing of personal information in transit accidentally;
• While performing system/network tuning, the aggregate of the traffic statistics should be used instead of collecting traffic on individual;
• Policy on acceptable use of Internet should be established by the employer for communicating to the employee.

Useful References

Office of the Privacy Commissioner for Personal Data, Hong Kong (December 2004), *Privacy Guidelines: Monitoring and Personal Data Privacy at Work*
(http://www.pcpd.org.hk/english/ordinance/files/monguide_e.pdf)
This document provides a full treatment of the Privacy Commissioner's views on workplace monitoring.

Data Protection Principles
(http://www.pcpd.org.hk/english/ordinance/ordglance1.html#dataprotect)

7.3 Direct Marketing

Overview

7.3.1 The following provides a general overview of how Information Communication Technology and computer data are used in the Direct Marketing industry.

Maintaining Personal Information Database

7.3.2 Business organisations that have a valuable clientele invariably maintain a database of the personal information of the customers. Customers' personal information is kept for the purpose of contacting customers, for customer surveys or for future product promotion. Further, in order to enhance customer loyalty by offering them more products and services, it is common for business organisations to share customers' personal information with business partners to provide non-competing products and services.

Collection of Data

7.3.3 The personal data of the customers are usually collected through voluntary submission. In order to attract customers to provide such data, it is common practice for some business organisations to offer discount or special offers to their customers as incentives for collecting their personal data.

7.3.4 There are times that the customers are providing such data for the purpose of after-sales services, such as maintenance of equipment, future upgrades of products, training etc.

7.3.5 The collection of these personal data can be through filling in forms, or through telephone conversation. Completed forms can be submitted online or by paper. It is important to understand that there are personal data being collected without going through any human interaction.

Data Storage and Retrieval

7.3.6 In conducting telemarketing activities or providing customer services, personal data are normally stored in computerised databases, and records will be selectively retrieved through data mining tools to create a subset of the database providing information for making customers contact. In the circumstances and faced with the operational constraints that these subsets of data need to be stored in portable storage devices (PSDs) such as smart cards, removable hard disks and USB memory drives, cautious steps must be taken to ensure the security of these data within such storage devices. The master copy of the database should always be kept at the organisation's computer system, and should never be stored in any PSDs.

7.3.7 The data may also be transmitted through network to terminals and displayed on screen for the purpose of providing information to the customer service officer to make contact with the customers.

Telemarketing

7.3.8 In cases whereby personal data are shared between organisations for the purpose of carrying out telemarketing, it is as important to the business organisation as well as to the individual consumer to make sure that these personal data are not disclosed to any other third parties, and that these data are protected from unauthorised access and use.

Compliance with PD(P)O

7.3.9 This section gives some practical guidelines from a technical perspective and management control perspective for enterprises conducting telemarketing operation, relevant to the compliance of the six DPPs.

Purpose and Manner of Collection of Personal Data (DPP1)

7.3.10 In general personal data are collected from the data subject through forms being filled in by the individual. These forms can be submitted in paper format or through electronic means such as online downloads, or through web pages. Some of the key considerations for the design and handling of these forms are:

- Must indicate clearly the mandatory elements or the optional elements to be supplied by the individual consumer.
- Must clearly describe in terms of the options for the individual how the data may be used. These terms and conditions must be presented so that they are easily readable by a person with normal eyesight.
- Must have a space for signature on the form for the individual to confirm his consent. In the case where information is collected through online forms, there should be a tick box available to the consumer to confirm that he has given the consent.
- The individual must have an option to maintain a copy of the information submitted. In cases where such information is to be submitted electronically, there should be a function on the web page where the individual can print out the form on a local printer.
- Where achievable, personal data should be collected and stored electronically in computer databases.
- It is good practice to reconfirm the data through recorded telephone conversation, and such confirmation can be archived as a record. In the process of “confirmation”, the caller must identify himself/herself and verify the identity of the called party, and the call must be carried out within a confidential environment.
- The full description of how and the scope within which the personal data would be used must be clearly specified on the appropriate web pages or in written format easily accessible by the individual.
- Only collect necessary information for the purpose of making contact with the individual, avoid recording of sensitive data such as HKID card number, passport numbers and PIN codes or unnecessary demographic information of individuals.

Accuracy and Duration of Retention of Personal Data (DPP2)

7.3.11 When collecting personal data from individual, the individual should be clearly informed as to the duration for which these data are to be kept. Such duration should be in line with the purpose of the data collection. For conducting each telemarketing campaign, data should be extracted into a subset just for the purpose of that particular campaign. Some of the key considerations for technical design and management control relating to this principle are:

- The database design should allow extract of sub sets of records for each campaign and each project, to be separately stored from the master database.
- For every project, identify the essential fields and only extract relevant records needed for the project.
- When subsets of data are created, and if there are any amendments or updates made in these subsets of data, appropriate synchronisation mechanism must be implemented to ensure data accuracy and the integrity of the master database.
- Always implant "phantom clients" within the data set for each project for traceability.
- An access log should be maintained for each record to provide traceability of when the record has been amended and when it has been extracted for use.
- In collecting personal data directly from customers during the direct marketing activity, if the information is being supplied through paper, one must ensure that the paper be shredded and that there is no risk in data leakage after the information has been stored electronically.
- After initial collection of personal data, it is good practice to reconfirm the data through recorded telephone conversation, and such confirmation can be archived as a record. In the process of "confirmation", effective and secure authentication of the identity of the caller as well as the called party is required to ensure a true confirmation.
- An opt-out list should be maintained and updated regularly of records of individuals who have indicated that they do not wish to be contacted for any marketing activities. This list may be kept as a general list or by market segments according to their expressed interest.
- There should be a mechanism to automatically obsolete a record after a specific expiry date.

Use of Personal Data (DPP3)

7.3.12 When personal data of a customer are to be used for carrying out telemarketing campaign, it is important to ensure that the product or service to be promoted is directly related to the service or product that the customer originally purchased, otherwise prescribed consent shall be obtained from the customer before carrying the campaign. Prudent management steps should be taken in case the purpose of use of these data has been changed from that of the original data collection. The following provides some technical guidelines for considerations:

- In the design of database in storing these personal data records, all personal data should be classified and stored in different records dependent on its classification. (For example, some data fields are classified as personal information, and some data fields may be classified as demographic type etc.) Common data fields should be segregated from sensitive data fields.

- Each data field should carry attributes for keeping information such as the security level, usage access right, expiry time of the usage etc. for each campaign.
- It is prudent management control to notify individual each time his data are being used for any purpose. When personal data are planned to be used for a purpose different from that of the original data collection or usage already agreed, it is essential to get consent from individual before the data are used.
- It is good practice to build up effective communication channels (SMS, email, or any other means of communications) between the enterprise and the individual for information exchange related to the use of his data.
- Each company must maintain a "do-not-call" list to record the request from individuals who wish not to be contacted at all or for any specific marketing activities.
- The do-not-call list, opt-in and opt-out list should be distributed to all staff members who undertake telemarketing activities with any subsequent changes and updates to the list being distributed by the most immediate means available through communication network.
- Referral to and strict observance of the do-not-call list is required at all times.

Security of Personal Data (DPP4)

7.3.13 Data security is of high importance in the design of the applications where personal data are stored and processed. It is important to implement strict management control to ensure that the personal data are secured and to comply with DPP4 Data Security Principle. The following provides some relevant guidelines for security considerations:

- In designing a database to hold these personal data, encryption should be applied to the data at database level.
- It is a good practice to design data penetration test plan for each call centre operation carrying out direct marketing activities, with the aim of using such test as a drill at defined period, and such test plan needs to be reviewed every now and then.
- Use "close network" for data processing and operational deployment (such as call station, integration with CIT network (Computer Integrated Telecommunication Network) etc.
- Avoid using PSDs that may have other intelligent programmes or secondary functions other than for data storage. In the case that there is such need to deploy these embedded function, it must be justified by a business purpose and authorised by designated authority.
- Consider using "thin client" approach utilising cloud computing technology for networks that are linked to multiple workstations. Avoid having data being transferred through the network by using remote access technology (e.g. Citrix, or M/S remote terminal services) whereby only the screen changes are being transferred through network, and data and application are being processed as an image inside the central server. This reduces the risk of having the data being hacked or hijacked during the transmission.
- Only enable I/O ports and peripherals that are essential to the processing needs for each terminal within the network.
- Classify all users that would have access right to the network based on the hierarchy of their data accessing and functional authority. Avoid allowing multiple logins per user.

7.3.14 Avoid as much as possible using PSDs such as USB Memory Sticks, iPods, MPs devices, notebooks, smart phones etc. for data storage. If these devices are to be deployed for data storage and transfer, the following issues need to be considered:

- Only PSDs authorised by management can be used within a network. Before authorising any PSD, security tests should be conducted to ensure that there are no other programmes that may cause external leakage of data preloaded on to these PSDs, and that the PSDs will only be used for data storage only.
- Anti-virus, malware, and Trojan scanning must automatically start as soon as a user log on to the network via desktop computers.
- Encryption algorithms used for encrypting data must allow for the recovery of encrypted data by an authorised person in case of forgotten password or change or departure of staff.
- Staff members are personally responsible for PSDs, as well as the data, in their care, and they must not share PSDs under any circumstances.
- Staff must not transport electronic storage devices that contain personal data via mail, internal mail, courier, post or other similar services.
- Data storage devices should always be in personal custody and should not be left unattended at all times whether in the office or otherwise.
- There must be a defined procedure for all staff to report any lost or stolen storage devices as a mandatory requirement.

7.3.15 In carrying out telemarketing activities, it is inevitable that personal data are being disclosed to and handled by different personnel, ranging from management to front line staff. These personnel should be made aware of the importance of data protection. Education and training should be provided to all staff involved in the telemarketing activities on the essence of PD(P)O and its DPPs, the security procedures in handling personal data including data loss (both actual or suspected) and data breaches or unauthorised data access, and their responsibilities to ensure personal data protection.

7.3.16 The following are some of the guidelines relating to this issue:

- Individuals taking on a job function along the work line should be told of the nature of personal data (not the content) to be disseminated to them to carry out their work.
- Each organisation should have a well-defined procedure in the handling of these data, and a mechanism to report any data loss or any abnormality discovered in the daily routine and process in the handling of these data.
- During each telemarketing campaign, there should be a “sign-in” and “sign-out” procedure for personnel using the personal data to understand and confirm the purpose for which the data are to be used for.
- This “sign-in” and “sign-out” procedures should be individual campaign based to avoid improper use of personal data, whether inadvertent or otherwise.

Information to Be General Available (DPP5)

7.3.17 DPP5 requires a data user to take reasonably practical steps to make known and be transparent about its policy and procedures that apply to its collection, retention and use of personal data.

7.3.18 The following are some suggested guidelines for compliance with DPP5:

- It is important for a data user to have a written policy statement, commonly referred to as Privacy Policy Statement (PPS) which states the kind of personal data held, and the various purposes for which personal data are being used or to be used.
- Business organisations should provide easy access for their customers either through Internet communications such as email or web pages, to their Privacy Policy Statement.
- For direct marketing organisations, it would be relevant to have the projects or marketing campaign which uses personal data described in their PPS, including details of the duration of the campaign and the purpose of such campaigns.
- It is a good practice to make prior announcement of any cross-marketing scheme to individuals whose personal data may be used.

Individuals' Rights of Access to and Correction of Their Personal Data (DPP6)

7.3.19 DPP6 provides individuals with the rights of access to and correction of their personal data.

7.3.20 For IT applications which collect and process personal data, there should be a logging sub-system to handle data access and correction requests, which should include such features as:

- Log the data when a data access/correction request is received and monitor related actions of compliance or refusal within the subsequent 40 days.
- Trigger the necessary response to the requestor in good time before the expiry of the 40-day period, and
- Create and maintain a log book on refusals to data access and correction requests and reasons for such refusals.

Useful References

Office of the Privacy Commissioner for Personal Data, Hong Kong (October 2010), *Guidance on the Collection and Use of Personal Data in Direct Marketing (http://www.pcpd.org.hk/english/publications/files/DM_e.pdf)*

Office of the Privacy Commissioner for Personal Data, Hong Kong (October 2011), *Guidance on the Use of Portable Storage Devices (http://www.pcpd.org.hk/english/publications/files/portable_storage_e.pdf)*

7.4 Biometrics

Definition

7.4.1 Biometrics refers to the measurement of physiological and behavioural characteristics used to identify computer users. Physiological characteristics commonly include the face, fingerprints, iris characteristics and DNA. Behavioural characteristics commonly include the way a person signs his/her signature, his or her voiceprint, and walk.

Applications

7.4.2 To use biometrics in identity authentication, an individual's physical characteristics (e.g. fingerprints, voice recording, eye iris scans, hand measurement) are captured to create a digital "map" (called a "template"). This is then stored by a security system and used later to authenticate the identity of the individual when he/she attempts to access the system.

7.4.3 Biometrics has gained wide usage in recent years. Examples of its use include:

Access Control

The user's (data subject) biometric characteristics, such as fingerprint, palm geometry or iris scan, are captured through a scanning device during the registration process (called an "enrolment"). Using a software algorithm, the scanned information is transformed into a "template", which is then stored in a computer system. When the individual attempts to gain access later, his/her biometric characteristics will be captured by the scanning device again. Access is granted if the scanned results closely match that on the computer system. In some installations, the biometric access control mechanism is supported by an additional piece of security device, such as a physical access card possessed by the individual.

Identity Authentication

An example is the e-channel border control operated by the Immigration Department in Hong Kong. A smart identity card is issued to each resident of Hong Kong. Biometric information (fingerprints and face photographs) is captured during the enrolment process of the smart identity card. Templates of the cardholder's thumbs are stored electronically in the chip of the smart Hong Kong Identity Card. When the smart identity card holder crosses the border through the e-channel, he/she inserts the identity card into the card reader at border control. The system validates the card and instructs the individuals to scan his/her thumb using the scanner at the e-channel station. This scanned result is then compared against the biometric information recorded in the card to authenticate the identity of the individual.

Automated Teller Machines (ATMs)

Some banks in the USA have implemented authentication systems for their ATMs using iris scan technology. During enrolment of the customer, his/her iris is scanned. A template of the iris is then created and stored in the computer system. On subsequent visits to use the ATM, the customer inserts the banking access plastic card. The system will perform a scan of the iris of the customer and then match with the digital image stored on the database. If they match, the customer's identity is authenticated and he/she can proceed to perform the banking transactions on the machine. In this process, the iris scan replaces the traditional personal identification number ("PIN") method to validate the identity of the customers. In some installations, the PIN is still required with the iris scan to add another layer of protection against fraudulent use of the ATMs.

7.4.4 Though many methods are used in biometrics measurement, fingerprints continue to be the predominant characteristics captured in biometric application due to its low implementation cost and high success rate in authenticating the users.

Possible Implications on Personal Data Privacy

7.4.5 Biometric information about individuals is stored in the form of digital template. It is regarded as personal data and is protected by PD(P)O of Hong Kong. Biometric data is considered sensitive due to its unchanging characteristics, in that they are not artificial information which can be rendered obsolete, and in no circumstances can an individual be disconnected from his unique biometric data. Companies planning to implement biometrics systems for their operations and business needs must understand and comply with DPPs and provisions of the PD(P)O. Compliance with these DPPs will ensure that applications using biometric data will not infringe the personal data privacy of individuals and that any captured biometric information is securely stored to prevent leakage and misuse. In any case, given the sensitive nature of biometric data, a data user should: (i) seriously consider whether collection of other less sensitive data may achieve the same purpose; (ii) consult the data subjects to be affected well in advance; and (iii) give the data subjects an option to supply other information instead of providing their biometric data.

7.4.6 Various complaint cases involving the use of biometric data have been reported to PCPD over the years. The Privacy Commissioner's views on one relevant case are described below.

7.4.7 In a complaint case in which an employer collected fingerprint data to record staff attendance, the Privacy Commissioner considered that the goal of collecting staff's attendance record effectively and accurately was not a sufficient ground for collection of fingerprint data. Since the employer had also installed surveillance cameras to monitor staff attendance and the system that collected fingerprint data also offered the option of using passwords for identification, the goal could also be achieved by those means without collecting the staff's fingerprint data. The Privacy Commissioner therefore decided that the collection of fingerprint data by the employer was unnecessary and excessive. The Privacy Commissioner also found that the employer might dismiss

the staff who did not cooperate in using the fingerprint attendance system, and the employer had not provided that staff with sufficient information to enable the staff to make an informed decision on whether to supply the data to the employer. In the circumstances, the Privacy Commissioner found that the employer's means of collecting the fingerprint data was unfair under DPP1(2)[1].

7.4.8 The Privacy Commissioner is of the view that under certain circumstances, involvement of biometric data may not necessarily consist of collection of such biometric data. For instance, an employer may wish to install a fingerprint recognition system which converts fingerprint image into a template and stores it in a smart card to be kept by the employee. The system verifies the employee by comparing and matching the template in the smart card and the fingerprint presented by the employee each time. The employer does not hold or have access to a copy of the employee's fingerprint image or template. Since the employer in such a case has not collected the employee's fingerprint data, the involvement of fingerprint data should not be regulated by PD(P)O.

Guidance Notes for IT Professionals in Biometrics Deployment

7.4.9 It is important for IT professionals, when proposing and designing computer systems using biometric technology, to adhere to DPPs. This is to ensure that the systems implemented will have the following privacy friendly characteristics:

- the purpose of the collection and use of the biometric data must be stated prior to or accompanying the data collection
- biometrics is used for a lawful purpose
- the biometric data is securely stored to avoid unauthorised or accidental access or use
- retention of the biometric data must not be longer than that is necessary for the purpose it is intended for
- use of the biometric data must be in conformance of original stated purpose. Deviation or extension of its use must not be carried out unless with the express and voluntary consent of the data subject
- Individuals have the right of data access to their biometric data and make request for data correction for perceived inaccuracies

7.4.10 Guidance notes for biometrics deployment are detailed under each DPP below. The text of the six principles stipulated by the Privacy Commissioner's office is quoted in square brackets [ ]. For a general treatment of each of DPPs in terms of definition and compliance relevant to system designers and operators, you are strongly advised to further refer to Chapter 6 for supplementary information.

[1] Report Number: R09-7884, from http://www.pcpd.org.hk/english/publications/files/report_Fingerprint_e.pdf

Purpose and Manner of Collection of Personal Data (DPP1)

7.4.11 [This provides for the lawful and fair collection of personal data and sets out the information a data user must give to a data subject on or before collecting personal data from that subject.]

Guidance Note

7.4.12 Biometric data should only be captured for a lawful purpose (e.g. crime investigation, legitimate business/security function like the identification of employees for accessing a specific area that requires close monitoring) that is related to the function or activity of the data user. Given the sensitive nature of biometric data, alternatives that are less privacy intrusive must first be explored and considered. When designing biometrics identification systems, personal data privacy protection and security safeguards must be included in the design of the system.

7.4.13 Biometric information should not be used as a universal unique identifier. A universal unique identifier facilitates the gathering of personal information from various databases in the system and can be a major threat to privacy if misused.

7.4.14 On the manner of collecting biometric personal data, the individuals (data subjects) involved should be explicitly informed what data is collected and for what purpose. Generally, the data subject should be provided an alternative to the supply of his biometric data. The data user should take appropriate steps to ensure that any consent from the data subject to the collection of his biometric data is genuine. This is particularly the case where the data subject (e.g. minor or employee) is in a weaker bargaining position than the data user. The process and any consent documentation involved must be well documented and disseminated to the data subject and kept by the data user. This ensures transparency of the data collection process and raises the awareness that the data collected is sensitive personal data which has to be protected.

Accuracy and Duration of Retention of Personal Data (DPP2)

7.4.15 [This provides that personal data should be accurate, up-to-date and kept no longer than necessary]

Guidance Note

7.4.16 The design of the system must ensure that the captured biometric information is accurate. An example is to capture the biometric data multiple times during enrolment to ensure its accuracy. In these multiple capture passes, the template generated in each pass must be compared for consistency.

7.4.17 Biometric data in an identifiable state (e.g. facial image, fingerprint or voice recording) should not be stored or used in a biometrics system other than for the purpose of generating the template. After the template is generated, the identifiable data should be completely destroyed, deleted or rendered useless. (The purpose of this action is to prevent the storage of fingerprints and facial images as opposed to fingerprint and facial recognition templates.)

7.4.18 On the retention of biometric data, this data must not be stored longer than is necessary for fulfilment of the purpose for which they are or are to be used. The retention period and the subsequent disposal/erasure of the captured data must be clearly defined and the procedures to be followed must be well documented. When the system using the data is no longer operational, specific user information must be completely destroyed, deleted or rendered useless.

Use of Personal Data (DPP3)

7.4.19 [This provides that unless the data subject gives express and voluntary consent otherwise personal data should only be used for the purposes for which they were collected or a directly related purpose.]

Guidance Note

7.4.20 As biometric data is sensitive personal information, its use must be the same as or directly related to the stated purpose of collection and use. Any change of use of the biometric data must have obtained the express and voluntary consent of the individuals concerned.

7.4.21 As a general rule, biometrics deployment should not be expanded to perform broader verification of identity related functions other than those originally intended. Any expansion or retraction of scope of use should be accompanied by full and public disclosure, and the oversight of an independent auditing body should be considered. Provision must be made for individuals to op-out of system usage in such situations.

Security of Personal Data (DPP4)

7.4.22 [This requires appropriate security measures to be applied to personal data (including data in a form in which access to or processing of the data is not practicable).]

Guidance Note

Storage

Biometric data must be stored in a secure manner to guard against unauthorised or accidental access, loss, erasure or other use. Normally, the biometric information is transformed into a template and stored in a database. The data should be encrypted to protect against unauthorised or accidental access and usage.

Security solutions must also be implemented to protect the database from accidental corruption, data loss or erasure.

Data Transmission

If the data has to be transmitted or transferred to another system, it should be encrypted to protect against leakage. Mechanism must be developed to ensure that the received data in such a transmission preserves its data integrity and accuracy.

After a biometrics comparison is made, the post-match decision transmission should be protected. Though these post-comparison decisions do not necessarily contain any biometric data, they will potentially contain personal data that can identify the data subject. The interception or compromise of these response messages could result in the leakage of personal information.

System Access
Access to biometrics system functions and data must be limited to restricted personnel, with explicit controls on usage and on export of data from the system. For highly sensitive data, checks and balances through access control requiring multiple users should be considered.

Segregation of Biometric Information
Biometric data should be stored separately from personal information, such as name, address, medical or financial data. This segregation can be physical (e.g. stored in separate locations on storage media) or logical (e.g. use security software to segregate access of biometric data from other personal information). The objective of this guidance note is to minimise the data privacy impact should the database be compromised.

Lifecycle Management
From a life cycle standpoint, biometric data must be protected at all stages of its lifecycle, including storage, transmission and matching. The techniques used can include encryption, use of private networks, installation in secure facilities, administrative controls and data segregation. For a given deployment, the protection used will be determined by a variety of factors, such as the location of the storage, location of matching activity, the type of biometrics involved, the capability of the biometrics system, which processes will take place in a trusted environment, and the risks involved should the data be compromised.

Information to Be Generally Available (DPP5)
7.4.23 [This provides for openness by data users about the kinds of personal data they hold and the main purposes for which personal data are used.]

Guidance Note

7.4.24 The purpose of collecting biometric data must be well documented so that both the data subject and the employees of the data user are fully aware of why the data is collected. The policy and practice in handling biometric data captured must also be well documented for the sake of transparency.

Access to Personal Data (DPP6)
7.4.25 [This provides for data subjects to have rights of access to and correction of their personal data.]

Guidance Note

7.4.26 Procedures should be developed to handle data access requests from individuals for their personal data. Procedures should also be developed to handle data correction requests for perceived inaccuracies of personal data.

7.4.27 In implementations where only the templates generated from the captured biometric data is stored (i.e. the source data is not retained after the enrolment process), the data access requestor should be made aware that the template cannot be used to re-generate the source biometric data.

Future Developments

7.4.28 Traditionally, biometrics systems compare a previously enrolled template with a "live" biometric data presented from the owner at the time of use/access. This model inevitably needs a copy of the biometric data (the template) to be stored in the system giving rise to issues related to the safekeeping and use of such personal data.

7.4.29 Recent developments in biometrics systems deploy a technique called **biometric encryption** which seeks to avoid storing the template altogether. With biometric encryption, the characteristics of biometric data, such as fingerprints, are used to generate a key which will in turn encrypt a secret message. As the biometric data such as a fingerprint must be presented each time to re-create the key to decrypt the secret message, biometric data is never stored in the system, thus avoiding the issues associated with storing biometric data. Although commercial products deploying biometric encryption is not common at the moment, the development in this area should be closely monitored as the technique appears to satisfactorily address both security and privacy concerns.

Useful References

Office of the Privacy Commissioner for Personal Data, Hong Kong (August 2007), *Guidance Note on Collection of Fingerprint Data*
(http://www.pcpd.org.hk/english/publications/files/Fingerprint_e.pdf)

Ann Cavoukian, Information and Privacy Commissioner of Ontario, Canada (November 2008), *Fingerprint Biometrics: Address Privacy Before Deployment*
(http://www.privacybydesign.ca/content/uploads/2008/11/fingerprint-biosys-priv.pdf)

Published by:

HONG KONG COMPUTER SOCIETY

Supported by:

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

Hong Kong Computer Society

LG1, No.78 Tat Chee Avenue, Kowloon Tong, Hong Kong

Tel: (852) 2834 2228 Fax: (852) 2834 3003

Email: hkcs@hkcs.org.hk Website: www.hkcs.org.hk