

# **Recommended Procedures for IT Practitioners on Personal Data Handling**

資訊科技從業員處理個人資料的建議程序

## **CONTENTS 目錄**

**FOREWORD**

前言

**INTRODUCTION**

引言

**PURPOSES OF THE RECOMMENDED PROCEDURES**

建議程序的目的

**RELATIONSHIP BETWEEN DATA USER AND IT STAFF**

資料使用者與資訊科技員工的關係

**RECOMMENDED PRACTICE FOR IT PRACTITIONERS**

建議措施

**FUNCTIONAL RESPONSIBILITIES OF IT STAFF**

資訊科技人員的職責

**DATA USER USING IT CONTRACTOR**

聘用資訊科技承辦商的資料使用者

**FURTHER CONSIDERATIONS IN THE USE OF ELECTRONIC DEVICE  
OR STORAGE MEDIA THAT STORES OR HANDLES PERSONAL DATA**

使用電子媒體儲存或處理個人資料的進一步考慮

**IMPLEMENTATION CONSIDERATIONS**

實施考慮

**RELATED GUIDELINES, STANDARD, POLICIES AND RESOURCES**

相關的指引、標準、政策及資源

## FORWARD

Public concern about IT security and the protection of personal data privacy grows rapidly in recent years due to the expanding volume of personal data collected and proliferating number of database containing our personal data. To assist IT professions across all sectors in better understanding the application of the Personal Data (Privacy) Ordinance in the handling of personal data, my Office has joined hands with IT professionals to develop a clear set of privacy compliant good practices encompassing management leadership, training, supervision and auditing.

This book outlines the procedures to be followed in circumstances in which personal data collected by a data user is accessed or processed by an IT contractor or sub-contractor appointed to work on some aspect of the system. Employers, IT professionals and system administrators are encouraged to embrace these guidelines and work to ensure their effective implementation. In combination good IT security procedures and good personal data privacy practices make for good governance. In turn, this is good for business and benefits our society in general.

Roderick B. Woo  
Privacy Commissioner for Personal Data

## 1. INTRODUCTION

### 1.1 PURPOSES OF THE RECOMMENDED PROCEDURES

Controls over personal data handling is part of good IT governance practices. The purpose of this document is to outline the professional responsibilities of IT practitioners and to provide guidance for others when using IT systems that contain or will be used for processing personal data. This guideline should be regarded as a supplement to, but not a substitute for, the relevant rules and regulations set by Office of the Privacy Commissioner for Personal Data (PCPD) that address the handling of personal data.

## 1.2 RELATIONSHIP BETWEEN DATA USER AND IT STAFF

Corporate or organization management should set up policies on the privacy aspect of personal data handling that data users<sup>1</sup> and IT staff should strictly observe. Data user should alert IT management when personal data is collected and stored in any of the IT systems or databases. IT staff should also report to the data user if any personal data will be used for any purpose that the data user was not aware of. The management may consider disciplinary action should any IT staff fail to observe the above-mentioned policies.

## 2. RECOMMENDED PRACTICE FOR IT PRACTITIONERS

### 2.1 FUNCTIONAL RESPONSIBILITIES OF IT STAFF

#### 2.1.1 Development staff

- If an application involves personal data, the application should generate a prominent notice at the start of the application.
- Real personal data should not be used for any kind of system testing.
- Personal data should not be used for system diagnosis or bug tracking. If system diagnosis or bug tracking is performed against personal data processing, masked or anonymised personal data should be used so that the individuals' identities in the personal data cannot be revealed.

#### 2.1.2 Database administrator

If the database contains personal data, the database administrator should be properly informed, and the procedures below should be followed by the database administrator:

- Database administrator should properly inform users when user accounts are set up that provide access to personal data.
- Applications that access personal data in the database should be documented and kept up-to-date.
- Database administrator should exercise proper controls and diligence at all stages of the routine and non-routine operations including but not limiting to:
  - Startup and access of the database
  - Export data from the database
  - Copy or backup of the database

---

<sup>1</sup> The term "data user" is defined in Personal Data (Privacy) Ordinance. 「資料使用者」的定義見《個人資料(私隱)條例》

### 2.1.3 Computer operators or system support staff

- Computer operators or system support staff should not have access to personal data unless formally approved.
- Computer operators or system support staff should be instructed not to access nor copy any personal data from the system.
- Computer operators or system support staff should ensure any media or hardware to be disposed of contains no personal data and has such data been deleted securely (that the data could not be recovered by any means).

### 2.1.4 Data entry personnel

- Data entry personnel should be restricted from unnecessary access to personal data stored in the system
- Data entry personnel should be informed if they are going to input personal data.
- Data entry personnel should be instructed not to retrieve nor copy any personal data from the system.

## 2.2 DATA USER USING IT CONTRACTOR

- Data user should select reputable IT contractor offering guarantees about its ability to ensure the security of personal data it handles.
- Data user should incorporate the following requirements in the service agreement with IT contractor:
  1. The security measures required to be applied by the contractor to protect any personal data that they may collect, view or use
  2. The prohibition of the contractor from using or disclosing personal data for any purpose not specified in the contract;
  3. The obligation on the part of the user and contractor to comply with the Data Protection Principles of the Personal Data (Privacy) Ordinance;
  4. The timely return of those personal data when they are no longer required for the IT contractor to provide its services, and timely deletion from the IT contractor's systems, and any backups;
  5. The timely reporting of any sign of abnormalities or security breaches in respect of those personal data;
  6. The Contractor should warrant that its staff have been properly trained in personal data handling.
- Data user should not release information that contains personal data to its IT contractor unless it is absolutely necessary for the IT contractor to complete the task.
- Data user should not release information that contains personal data to its IT contractor for the purpose of systems testing.
- Data user should clearly inform its IT contractor whenever the IT contractor is going to carry out any task that involves the handling of personal data, its responsibility in maintaining the privacy of the personal data, such as application systems development, database processing, data conversion, etc.

- Information that passed from the data user to its IT contractor that contains personal data should contain proper label.
- Data user should keep track and proper records of all the personal data that has been given to its IT contractor.
- Data user should assess the IT contractor from time to time to confirm that it is carrying out the required security measures and obligations in handling the personal data given to it.
- Data user should ensure that the IT contractor carries out appropriate checks on their staff who handle the personal data.
- Data user should give clear instructions to the IT contractor in respect of the use, transmission, storage and destruction of the personal data given to it.
- There should be no sub-contracting without explicit consent of data user if the sub-contracting will involve processing or using of personal data.
- IT contractor must be responsible for the sub-contractor's conduct relating to personal data handling.
- Data user may choose to deal directly with sub-contractors but the same controls shall be applied as above.
- Data user should consider issuing security requirement document(s) to and request respective signed undertaking from the sub-contractor.

## 2.3 FURTHER CONSIDERATIONS IN THE USE OF ELECTRONIC DEVICE OR STORAGE MEDIA THAT STORES OR HANDLES PERSONAL DATA

### 2.3.1 Accessing personal data in the database

- All access to personal data in the database should be authorized, monitored and accounted for.
- All database copy/backup from database that contains personal data should be authorized, monitored and accounted for.
- All database image exported from database that contains personal data should be authorized, monitored and accounted for.
- Reports on the above database operations should be produced and reviewed regularly.

### 2.3.2 Accessing personal data in file

All files containing personal data should be properly protected, identified, monitored, and handled by authorized personnel only.

### 2.3.3 IT systems that access personal data

- Prominent notice should be generated whenever an end user accesses an IT system that contains personal data.
- End users of an IT system should not export or save any personal data from the system unless formally approved.

If an IT system is going to access personal data, proper notice should be included in the IT system user guides and manuals and the access should be monitored and accounted for.

### 2.3.4 Exported data

- Export of personal data should be authorized.
- Exported personal data on portable storage media, e.g. floppy diskettes, optical discs, USB drives, should be properly labeled and stored.
- Computer printed copy that contain personal data should contain proper label and stored.
- Email that contains or attached with personal data should have the content encrypted and be properly labeled.

### 2.3.5 Retention period / Personal data destruction

- The retention period and conditions for personal data destruction should be specified by system/data owner.
- Whenever the personal data is no longer used, it should be destroyed properly.
- The retention period of personal data in IT systems should follow the relevant legal and regulatory requirements, and the industry standards. Where there is no specific legal or regulatory requirements or industry standard applicable to the organization, the personal data in the system should be destroyed as soon as possible.
- For personal data within a personal computing device (including PDA, smartphone, netbook notebook, etc.), its storage media or hard disk should be sanitized or destroyed.
- For personal data in a network computing or storage device (including NAS, SAN system, server, etc.), its hard disk should be sanitized or destroyed.
- All backup copies and exported copies should be destroyed securely.
- All printed copies should be destroyed securely.
- Proper records should be kept of the destructions.

### 2.3.6 System assessment on personal data

- Creation, access, modification, destruction of any personal data record stored in electronic device or storage media should be assessed periodically and documented.

## 3. IMPLEMENTATION CONSIDERATIONS

3.1 This Guideline is meant to be technology neutral, and hence its adoption will need to be tailored to the requirements and circumstances of the individual organization and its specific technology environment.

3.2 Different organizations have different security needs, and governed by different regulatory requirements. Therefore, risk assessments are recommended practices for the individual organization to determine the extent of security measures required for its own environment.

3.3 It is also a recommended best governance practice that all controls and procedures be documented and kept up to date.

## 4. RELATED GUIDELINES, STANDARDS, POLICIES AND RESOURCES

### 4.1 Related Policies

- Personal Data (Privacy) Ordinance (<http://www.pcpd.org.hk/english/ordinance/ordfull.html>)
- Data Protection Principles (<http://www.pcpd.org.hk/english/ordinance/ordglance1.html#dataprotect>)

### 4.2 Related Guidelines

Pop-up Message/Notice and Printed Label

**Sample:**

“This database is gathered for the purposes of XXXXX. It contains “Personal Data” as defined in the Personal Data (Privacy) Ordinance (Cap. 486) and must be treated by all users according to the six Data Protection Principles (DPPs) as contained in Schedule 1 to the Ordinance (<http://www.pcpd.org.hk/english/ordinance/ordglance1.html#dataprotect>). Personal data in this database must not be used for any purpose other than that for which they were originally collected. Once the data contained in this database or printed reports have ceased to service their legitimate purpose, they must be appropriately destroyed.”

**4.3 Related Resources**

- PCPD Codes of Practice/Guideline (<http://www.pcpd.org.hk/english/ordinance/codes.html>)
- Control Objectives for Information and related Technology (COBIT) (<http://www.isaca.org/cobit>)

October 2006

February 2009 (First Revision)