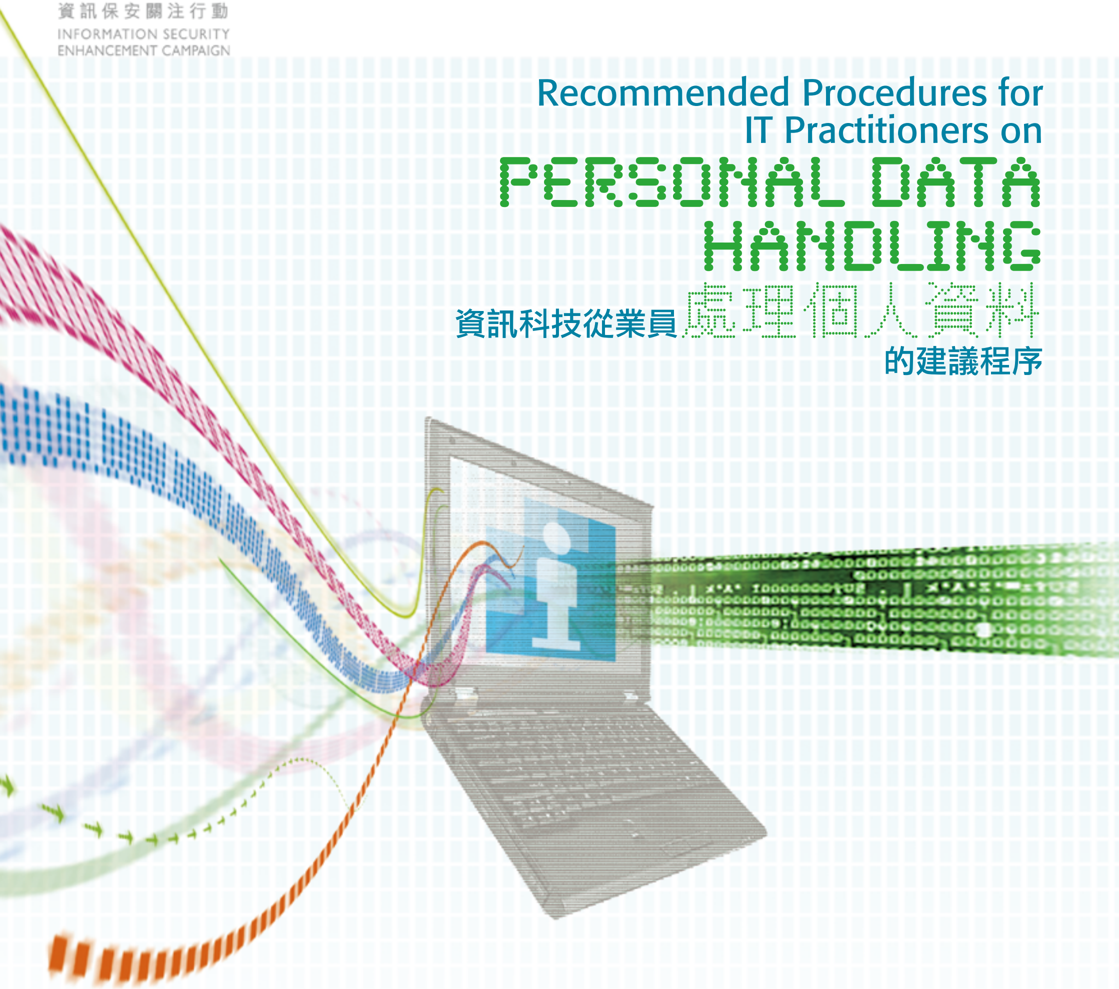
ISEC
資訊保安關注行動
INFORMATION SECURITY ENHANCEMENT CAMPAIGN

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



Published by:
出版機構：

iProA Internet Professional Association 互聯網專業協會

ISACA Serving IT Governance Professionals Hong Kong Chapter

香港工程師學會 THE HONG KONG INSTITUTION OF ENGINEERS

Supported by:
支持機構：

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

CONTENTS 目錄

FOREWORD

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

前言

近年，由於被收集的個人資料數量日益龐大，載有個人資料的資料庫數目日漸增多，社會大眾越來越關注資訊科技及個人資料私隱的保障。為了協助各行業的資訊科技從業員清楚了解如何在處理個人資料時遵從《個人資料（私隱）條例》的規定，公署與資訊科技專業人員制定了一套有關保障私隱的良好行事方式，可以應用於行政管理、培訓、督導及審核方面。

本書概述了受聘處理電腦系統某範疇的資訊科技承辦商或分判商，在存取或處理資料使用者所收集的個人資料時應遵從的程序。僱主、資訊科技專業人員及系統管理人員應把這些指引納入工作中，並確保有效施行。良好的資訊科技保安措施結合良好的個人資料私隱行事方式，可達致良好的管治效果。這不僅有利商業發展，亦令社會大眾得益。

吳斌
個人資料私隱專員

1. INTRODUCTION

1.1 PURPOSE 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[1] and IT staff should strictly observe. Data user should alert IT management when personal data is collected and stored in any of the IT

1. 引言

1.1 建議程序的目的

監控個人資料的處理在資訊科技業方面屬於良好管治措施的一部分。本文旨在概述資訊科技從業員的專業職責，並為其他人士提供使用資訊科技系統(其系統載有個人資料或將會用作處理個人資料)的指引。本指引是個人資料私隱專員公署為處理個人資料而制定的規則及規例以外的增補，而非替代有關條文。

1.2 資料使用者與資訊科技員工的關係

公司或機構的管理層應制定處理個人資料的私隱政策，而資料使用者[1]及資訊科技人員則應嚴格遵守。如資料使用者在資訊科技系統或資料庫收集及儲存個人資料，應該通知資訊科技管理層。如

[1] 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》

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.
- 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 personal data is the ONLY available information for system diagnosis or bug tracking, the personal data should be masked so that the individuals' identities in the personal data cannot be reviewed.

個人資料將會使用於資料使用者不知道的用途，資訊科技人員亦應向資料使用者報告。如資訊科技人員沒有遵守上述政策，管理層會考慮採取紀律行動。

2. 建議措施

2.1 資訊科技人員的職責

2.1.1 開發人員

- 如應用程序涉及個人資料，在該應用程序啟動前，應發出顯眼的通知。
- 個人資料不應使用於任何系統測試。
- 個人資料不應使用於系統診斷或錯誤追蹤。如**只有**個人資料是用作系統診斷或錯誤追蹤，應遮蓋有關資料，令人無法得悉資料中個別人士的身份。

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.
- 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

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.

2.1.2 資料庫管理員

如資料庫載有個人資料，資料庫管理員應獲得適當的通知，並依從下列程序：

- 資料庫管理員建立可以存取個人資料的使用者帳戶時，應妥善地通知使用者。
- 在資料庫存取個人資料的應用程序，應記錄存檔。
- 資料庫管理員在例行及非例行操作中的各個階段，均應作出適當的監控並謹慎處理，各個階段包括但不限於：
  - 啟動及進入資料庫
  - 從資料庫輸出資料
  - 複製資料庫或為資料庫備份

2.1.3 電腦操作人員或系統支援人員

- 電腦操作人員或系統支援人員除非正式獲得批准，否則不得存取個人資料。
- 電腦操作人員或系統支援人員應獲指示，不得在系統內存取或複製任何個人資料。

2.1.4 Data entry personnel

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

2.2 DATA USER USING IT CONTRACTOR

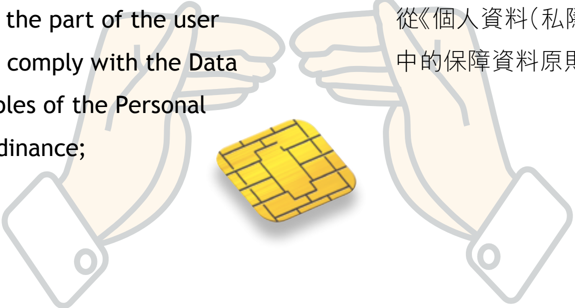
- Data user should select reputable IT contractor offering guarantees about its ability to ensure the security of personal data it handles.
- Data user should incorporate the following requirements in the service agreement with IT contractor:
  1. The security measures required to be applied by the contractor 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;

2.1.4 資料輸入人員

- 如資料輸入人員將要輸入個人資料，他們應得到通知。
- 資料輸入人員應獲指示，不得在系統內存取或複製任何個人資料。

2.2 聘用資訊科技承辦商的資料使用者

- 資料使用者應揀選信譽良好、能保證安全處理個人資料的資訊科技承辦商。
- 資料使用者應在與資訊科技承辦商簽訂的服務合約中加入下列要求：
  1. 列明承辦商必須採取的保安措施，以保障他們可能收集、看到或使用的個人資料；
  2. 承辦商不得為合約無訂明的目的而使用或披露個人資料；
  3. 使用者及承辦商有責任遵從《個人資料(私隱)條例》中的保障資料原則；



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.

4. 承辦商不再需要以該等個人資料來提供服務時，應適時地交還資料，並從其系統中刪除資料及備份；
5. 承辦商必須及時報告該等個人資料的不尋常徵兆或保安違規情況；
6. 承辦商應保證其員工在處理個人資料方面，已接受適當的培訓。

- 資料使用者不應向資訊科技承辦商發放載有個人資料的資訊，除非承辦商絕對需要這些資訊才能完成工作。
- 資料使用者不應向資訊科技承辦商發放載有個人資料的資訊，以進行系統測試。
- 資料使用者應清楚通知資訊科技承辦商，當承辦商進行任何涉及處理個人資料的工作時，例如開發應用系統、處理資料庫、轉換數據等，承辦商是有責任保持個人資料的私隱。

- Information that passed from the data user to its IT contractor that contains personal data should contain proper label.
- 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 keep track and proper records of all the personal data that has been given to its IT contractor.
- 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.

- 資料使用者將載有個人資料的資訊交給資訊科技承辦商時，資訊應包含適當的標籤。
- 資料使用者應不時審核資訊科技承辦商，以確定承辦商在處理收到的個人資料時執行了所需的保安措施及履行了責任。
- 資料使用者應確保資訊科技承辦商會向處理個人資料的員工進行適當的檢查。
- 資料使用者應為交給資訊科技承辦商的所有個人資料保存適當的記錄。
- 資料使用者應就資訊科技承辦商在使用、傳輸、儲存及銷毀所收到的個人資料，向承辦商發出清晰的指示。
- 如分判工作涉及處理或使用個人資料，在得到資料使用者的明確同意之前，不得把工作分判。
- 資訊科技承辦商必須對分判商處理個人資料的行為負上責任。
- 資料使用者可選擇與分判商直接聯絡，但必須採取上述同樣的監控措施。

2.3 FURTHER CONSIDERATIONS IN THE USE OF ELECTRONIC 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 使用電子媒體儲存或處理個人資料的進一步考慮

2.3.1 存取資料庫的個人資料

- 凡在資料庫存取個人資料，都應獲得授權、受到監察，以及作出解釋。
- 凡複製載有個人資料的資料庫複本／備份，都應獲得授權、受到監察，以及作出解釋。
- 凡從載有個人資料的資料庫輸出圖樣，都應獲得授權、受到監察，以及作出解釋。
- 有關上述的資料庫運作報告，應定期編製及審核。

2.3.2 存取檔案的個人資料

所有載有個人資料的檔案應妥為保護、分辨、監察，以及只限由獲授權人員處理。

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 guide, 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 removable storage media, e.g. floppy diskettes, CDs, USB drives, should be properly labeled.
- Computer printed copy that contain personal data should contain proper label.
- Email that contains personal data should have the content encrypted and properly labeled.

2.3.3 存取個人資料的資訊科技系統

- 每當終端用戶進入載有個人資料的資訊科技系統時，系統應發出顯眼的通知。
- 除非獲得正式批准，否則資訊科技系統終端用戶不應由系統輸出或儲存任何個人資料。

如資訊科技系統將會存取個人資料，資訊科技系統用戶指引應包括適當的通知，而存取資料應受到監察，以及作出解釋。

2.3.4 輸出的資料

- 輸出個人資料應獲得授權。
- 輸出的個人資料如儲存於可移動媒體，例如：軟磁碟、光碟、通用串列匯流排(USB)驅動器，應加上適當的標籤。
- 載有個人資料的電腦列印複本應包含適當的標籤。
- 載有個人資料的電子郵件內容應加密及加上適當的標籤。

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 PC, the PC's hard disk should be sanitized.
- For personal data in a server, the server's hard disk should be sanitized.
- All backup copies and exported copies should be destroyed.
- All printed copies should be destroyed.
- Proper records should be kept of the destructions.

2.3.5 個人資料的保留期／銷毀

- 系統／資料擁有人應明確規定個人資料的保留期及銷毀條件。
- 如個人資料不會再使用，應適當地予以銷毀。
- 資訊科技系統的個人資料保留期應依從有關的法律及規管性規定及行業標準。如沒有對該機構適用的特定法律或規管性規定或行業標準，系統內的個人資料應盡快予以銷毀。
- 至於個人電腦內的個人資料，個人電腦的硬碟應清除乾淨。
- 至於伺服器內的個人資料，伺服器的硬碟應清除乾淨。
- 所有備份複本及輸出複本應予以銷毀。
- 所有列印複本應予以銷毀。
- 銷毀記錄應適當地保存。

2.3.6 System assessment on personal data

- Creation, access, modification, destruction of any personal data record stored in electronic 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.

2.3.6 個人資料的系統審核

- 在電子媒體建立、存取、修改及銷毀個人資料記錄，應予以定期審核，並記錄存檔。

3. 實施考慮

3.1 本指引是科技中立的。因此，在採用本指引時，需要按個別機構的要求和情況，以及其特定的技術環境作出修改。

3.2 不同的機構有不同的保安需要，並由不同的規管性規定管限。因此，個別機構應作出風險評估，按其環境決定所需的保安措施。

3.3 另一個建議的理想管理措施是把所有的監控過程及程序記錄存檔，並不斷更新。

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

4. 相關的指引、標準、政策及資源

4.1 相關政策

- 《個人資料(私隱)條例》(http://www.pcpd.org.hk/chinese/ordinance/ordfull.html)
- 保障資料原則 (http://www.pcpd.org hk/chinese/ordinance/ordglance1.html#dataprotect)

4.2 相關指引

自動彈出的訊息／通告及列印的標籤

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."

樣本：

「本資料庫設立的目的是XXXXX。

它載有《個人資料(私隱)條例》(第486)所界定的「個人資料」，所有用戶必須按照條例附表1所載的六項保障資料原則處理有關資料(http://www.pcpd.org.hk/chinese/ordinance/ordglance1.html#dataprotect)。本資料庫的個人資料不得用於原本的收集目的以外之目的。當本資料庫或列印報告中的資料的合法用途終止時，有關資料必須適當地予以銷毀。」

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)

4.3 相關資源

- 個人資料私隱專員公署的實務守則／指引（http://www.pcpd.org.hk/chinese/ordinance/codes.html）
- 資訊及相關技術的控制目標（COBIT）（http://www.isaca.org/cobit）

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

URL: www.pcpd.org.hk

Email: enquiry@pcpd.org.hk

Tel: 2827 2827

Fax: 2877 7026

Address: 12/F, 248 Queen's Road East,
Wanchai, Hong Kong
香港灣仔皇后大道東248號12樓

ISACA®
Serving IT Governance Professionals
Hong Kong Chapter

URL: www.isaca.org.hk

Email: info@isaca.org.hk

Tel: 8101 2801

Fax: 8101 2802

Address: 15B Yam Tze Commercial
Building, 23 Thomson Road, Wanchai,
Hong Kong
香港灣仔譚臣道23號王子商業大廈
15樓B室

iProA
Internet Professional Association
互聯網專業協會

URL: www.iproa.org

Email: iproa@iproa.org

Tel: 2778 0040

Fax: 2778 0032 / 3157 1320

Address: iBay, Level 10, Cyberport 2,
100 Cyberport Road, Hong Kong
香港數碼港道100號數碼港
第2座10樓iBay

THE 香港 HONG KONG INSTITUTION
工程師學會 OF ENGINEERS

URL: www.hkie.org.hk

Email: hkie-sec@hkie.org.hk

Tel: 2895 4446

Fax: 2577 7791

Address: 9/F Island Beverley,
No 1 Great George Street,
Causeway Bay, Hong Kong
香港銅鑼灣記利佐治街1號金百利9樓

October 2006
2006年10月