

Hong Kong Institute of Human Resource Management

Learning & Development Seminar

HKIHRM Office, Causeway Bay, Hong Kong

4 October 2016

Data Privacy and Security Challenges

Presented by

Employees Using Own Mobile Devices

Stephen Kai-yi Wong

Privacy Commissioner for Personal Data, Hong Kong



20



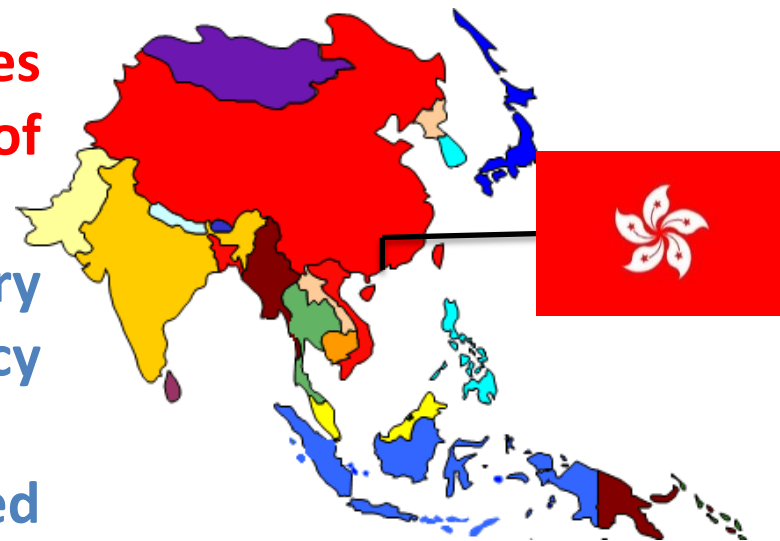
PCPD.org.hk

est. 1996

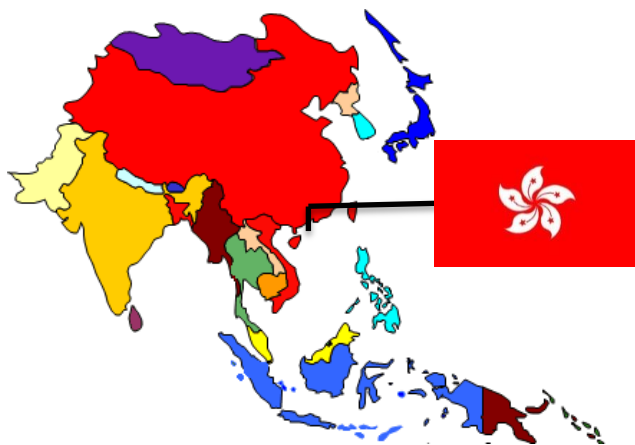
香港個人資料私隱專員公署
Privacy Commissioner
for Personal Data, Hong Kong

Personal Data (Privacy) Ordinance – No Stranger to HR Managers

- comprehensive and stand-alone
 - covering the public (government) and private sectors
- referenced to **OECD Privacy Guidelines** and **EU Data Protection Directive of 1995**
- enforced by an independent statutory regulatory body – the Privacy Commissioner for Personal Data
- named the second most trusted complaint handling agencies in Hong Kong



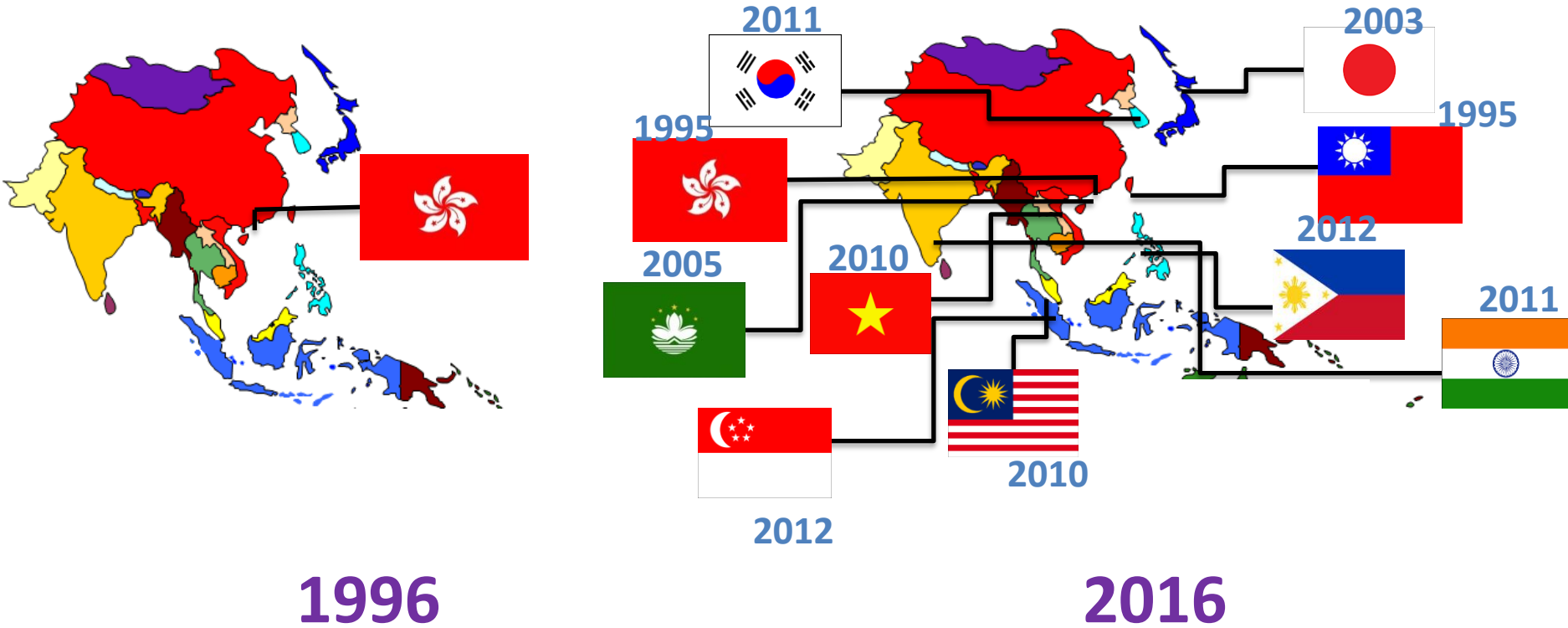
More Asian Jurisdictions Will Implement Similar Laws



1996

3

More Asian Jurisdictions Will Implement Similar Laws



The Six Data Protection Principles of the Ordinance

6 保障資料原則 Data Protection Principles

PCPD.org.hk

1 收集目的及方式 Collection Purpose & Means



資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應直接與其職能或活動有關。

須以切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移給哪類人士。

收集的資料是有實際需要的，而不超乎程度。

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function/activity of the data user.

All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred.

Data collected should be necessary but not excessive.

2 準確性儲存及保留 Accuracy & Retention



資料使用者須確保持有的個人資料準確無誤，資料的保留時間不應超過達致原來目的的實際所需。

Personal data is accurate and is not kept for a period longer than is necessary to fulfill the purpose for which it is used.

3 使用 Use



個人資料只限用於收集時述明的目的或直接相關的目的，除非得到資料當事人自願和明確的同意。

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

4 保安措施 Security



資料使用者須採取切實可行的步驟，保障個人資料不會未經授權或意外地被查閱、處理、刪除、喪失或使用。

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

5 透明度 Openness



資料使用者須公開其處理個人資料的政策和行事方式，交代其持有的個人資料類別和用途。

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

6 查閱及更正 Data Access & Correction



資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

A data subject must be given access to his personal data and to make corrections where the data is inaccurate.

5

The Six Data Protection Principles of the Ordinance

《 個人資料(私隱)條例 》下的

六項保障資料原則



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

保障、尊重個人資料
Protect, Respect Personal Data

PCPD.org.hk

PCPD



H.K.

20



PCPD.org.hk

est. 1996

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

Hong Kong's Personal Data (Privacy) Ordinance

Main points and mandates:

- the law is not prohibitive, rather it is facilitating
- principle-based that allows for flexibility and adaptability
- protection needs to be secured through:
 - fair enforcement
 - compliance monitoring
 - promotion and awareness driving
- protection without compromising the interests of all stakeholders including:
 - individuals
 - data users/controllers
 - government



Digital Footprint Protection is the Biggest Challenge

這個年代，上網就必然會留下數碼腳印！



20



PCPD.org.hk

est. 1996

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

Digital Footprints Are Stored in All Forms and in Many Types of Devices

Digital footprints may consist of:

- browsing history and behaviours
- email messages and photos taken
- travel plans, calendar and contact details

Traditionally such data is stored in desktop computers but now it is mostly in mobile devices

Using personal mobile devices for work combines the risk of (1) data breach of organisation-collected personal data and (2) leakage of private information of individuals and their family members...

9

Types of Mobile Devices

Portable storage devices:

- mainly USB memory and similar storage devices
- risks = loss of device with unencrypted personal data stored

Smart devices:

- mainly smartphones and tablets
- risks = loss of device with persona data, eavesdropping of data transmitted, access of data by other apps and intrusion of personal data belonging to the device owner

10

Portable Storage Devices

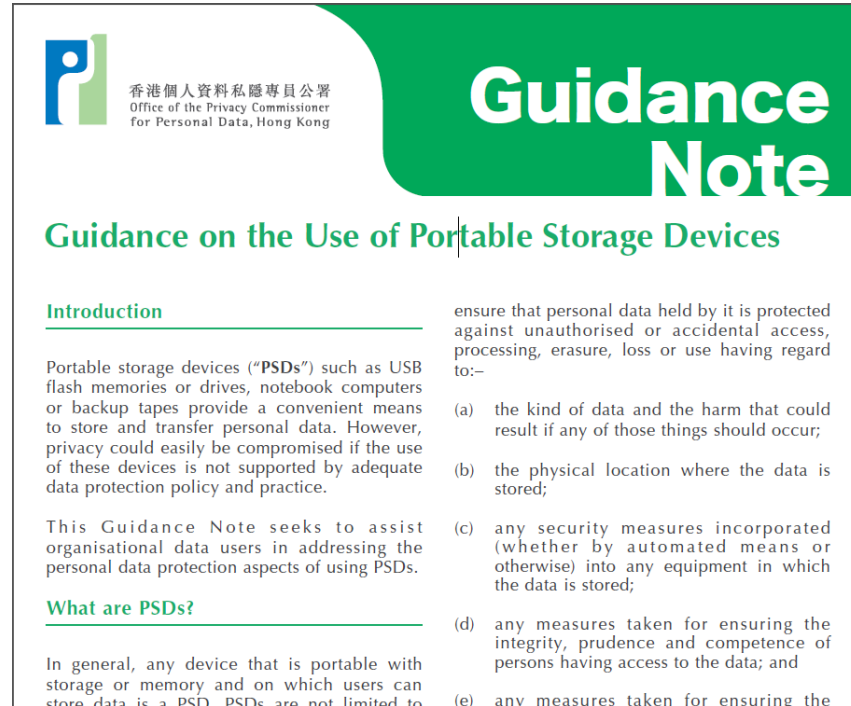
- loss of portable storage devices remains a prime concern



Year	2012	2013	2014	2015	2016 (up to August)
Number of cases reported	11	10	5	8	9
Individuals affected	6,552	4,492	478	211,704	28,906

Portable Storage Devices

- Privacy Commissioner published *Guidance on the Use of Portable Storage Devices* to provide best practice for organisations using USBs, etc.



The image shows the cover of a guidance note. At the top left is the PCPD logo (a stylized 'P' in a blue and green square) and the text '香港個人資料私隱專員公署 Office of the Privacy Commissioner for Personal Data, Hong Kong'. To the right, the title 'Guidance Note' is written in large white letters on a green background. Below this, the subtitle 'Guidance on the Use of Portable Storage Devices' is written in green. The main content is divided into two columns. The left column has a green header 'Introduction' followed by a paragraph: 'Portable storage devices ("PSDs") such as USB flash memories or drives, notebook computers or backup tapes provide a convenient means to store and transfer personal data. However, privacy could easily be compromised if the use of these devices is not supported by adequate data protection policy and practice.' Below this is another green header 'What are PSDs?' followed by a paragraph: 'In general, any device that is portable with storage or memory and on which users can store data is a PSD. PSDs are not limited to'. The right column contains a paragraph: 'ensure that personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use having regard to:-' followed by a list of five items (a) through (e) detailing security measures.

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

Guidance Note

Guidance on the Use of Portable Storage Devices

Introduction

Portable storage devices ("PSDs") such as USB flash memories or drives, notebook computers or backup tapes provide a convenient means to store and transfer personal data. However, privacy could easily be compromised if the use of these devices is not supported by adequate data protection policy and practice.

This Guidance Note seeks to assist organisational data users in addressing the personal data protection aspects of using PSDs.

What are PSDs?

In general, any device that is portable with storage or memory and on which users can store data is a PSD. PSDs are not limited to

ensure that personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use having regard to:-

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

Guidance on the Use of Portable Storage Devices

- **avoidance**

- controls types of devices, circumstances of use and types/amount of personal data stored

- **prevention**

- encrypt data stored so data is not lost even when the device is lost

- **detection**

- inventory control to ensure accountability by employees
- data breach notification and handling process in place to limit damage



Smart Device – Recent Developments

- number of world-wide mobile users surpasses desktop users in 2014
- more Google searches were carried out from mobile than desktop in 2015
- there are over 14 millions active SIM cards in use in Hong Kong
- the Hong Kong Monetary Authority removed restriction from banks to use Bring Your Own Device (BYOD) in 2014



Bring Your Own Device (BYOD)

- increasingly common for organisations to allow employees to use their own mobile devices (e.g. smartphones, tablets) to access and work with organisational information
- organisational information may contain personal data
- use of own devices must therefore comply with the privacy law



BYOD Information Leaflet

- issued in August 2016
- highlights personal data privacy risks
- suggests best practices



Bring Your Own Device (BYOD)

Executive Summary

Bring your own device (“BYOD”) is an organisational policy that allows employees to use their own mobile devices to access the organisation’s information, including personal data collected by the organisation. For the purpose of this leaflet, personal data collected by an organisation is referred to as “organisation-collected personal data”.

BYOD Risks – Overview

most relevant risks are:

- lack of control that leads to:
 - over-retention of personal data (DPP2)
 - change of use and transfer (DPP3)
 - security breaches (DPP4)
 - non-fulfilment of data access requests (DD6)
- access to private/personal information stored by employees in the BYOD:
 - direct purpose and lawful collection (DPP1)



Retention of Personal Data

- points to note:
 - whether personal data should be retained in BYOD equipment
 - whether and how the organisation's retention policy can be applied equally and effectively to personal data stored in BYOD equipment (e.g. explicitly extend the policy to BYOD equipment?)



Use of Personal Data

- point to note:
 - organisations should devise policies, establish controls and remind employees to ensure that data stored in BYOD equipment is not used for a new purpose without prescribed consent



Security of Personal Data

- points to note:
 - BYOD equipment may store employees' personal/private data
 - consider employees' own privacy when applying the organisation's security policy to BYOD equipment (e.g. remotely accessing BYOD equipment to track its location may infringe employees' privacy)



Security of Personal Data



- points to note:
 - protect the personal data stored in BYOD instead of the device itself:
 - prevent data from being stored in the BYOD (e.g. use BYOD to remote access data stored centrally)
 - apply access control to the personal data stored (e.g. addition level of username/password is required to access the data so that family members cannot see the data by accident)
 - encrypt personal data stored (e.g. if data is accessed by other apps the data cannot be interpreted)

21

Data Access Right

- points to note:
 - organisations should establish procedures to comply with data access/correction requests particularly for data stored only in BYOD
 - Consider the need to backup data stored in BYOD but not centrally



Best Practices of Implementing BYOD

- establish policy
- conduct risk assessment
- apply technical solutions
- monitor and review



Establish BYOD Policy

- respective roles, obligations and responsibilities of the organisation and employees
- criteria for deciding what information are accessible by BYOD, and what type of BYOD is allowed



Establish BYOD Policy

- technical solutions applied to protect the organisation's and employees' personal data
- mechanisms for the organisation to monitor compliance with BYOD policy and consequences of non-compliance



Conduct Risk Assessment

- assess sensitivity of personal data involved and the harm of breaches
- develop proportionate access controls and security measures
- cover both the organisation's personal data and employees' private data
- may seek assistance from contractors for risk assessment and solution, but still accountable for privacy breaches caused by contractors



Apply Technical Solutions

- typical mobile device controls include:
 - remotely wipe or lock BYOD equipment
 - detect whether BYOD equipment is “jailbroken” or infected with malware
 - record websites visited
 - lock or delete data if incorrect passwords are entered repeatedly
- but all of these may be seen as a way of monitoring employees at and off work...



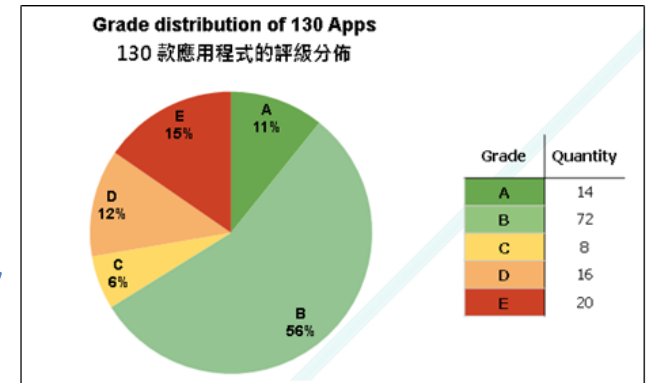
Apply Technical Solutions

- alternative technical solutions may include :
 - implement additional log-on for accessing organisational data so family members cannot do so accidentally
 - enforce complex passwords for accessing organisational data
 - independently encrypt data stored and transmitted by the app so the hackers need to compromise both the device and the app to gain access to the data
 - auto-erase data when multiple unsuccessful log on or lost of device is detected



Apply Technical Solutions

- know how to encrypt data:
 - in a 2015 HKCER study of 133 mobile apps transmitting personal data, 33% of them did not apply encryption properly and data could be intercepted by fake Wi-Fi access point



29

Monitoring and Review

- organisations should regularly review and update BYOD policy following technological or business changes:
 - e.g. changes to nature and sensitivity of personal data stored in BYOD equipment may require updating BYOD policy



Privacy by Design



- employees may be given apps to run on BYOD for work purpose but they can also track people out of office hour
- Privacy by Design:
 - tracking ability should be off during out of office hour or outside work place
 - employee may switch tracking off

Monitoring and Personal Data Privacy at Work

- the need for monitoring must be evaluated:
 - Assess whether there is genuine need for monitoring
 - find out if there are any Alternatives
 - Accountable with policy and compliance measures in place



Monitoring and Personal Data Privacy at Work

- the monitoring process must be managed well:
 - Clarity in the scope and purpose in the monitoring policy
 - clear Communication with employees on the policy
 - Controls in place for the holding, processing, use and disclosure of data



Data Privacy and Security Challenges presented by Employees using own Mobile Devices

