

The Hong Kong Institute of Directors  
Speaker Luncheon Meeting  
25 August 2022

# Data Privacy Pitfalls and Tips for Directors

**Ada CHUNG Lai-ling**  
Privacy Commissioner for Personal Data



# Data Privacy Pitfalls for Directors

# Data Breach Is on the Rise: Major data breaches in recent years and individuals affected

2020	Estée Lauder	440 million
	Microsoft	250 million
	Instagram, TikTok, Youtube	235 million
2019	Capital One (Bank)	160 million
	Zynga (Online game developer)	218 million
	Facebook	419 million
2018	Marriott Hotel	383 million
	Twitter	330 million
	Facebook	140 million
	Uber	57 million
	Cathay Pacific Airways	9.4 million

Reference: Nord VPN, Forbes

# Major Data Breaches in 2021

Platforms	Affected individuals	Individuals in Hong Kong
Facebook	533 million	2.93 million
LinkedIn	500 million	280,000 (All Hong Kong users)
Air India	4.5 million	Unknown

# Notable Data Breaches in 2022

## Harbour Plaza Hotel Management Limited

- A local hotel group operating **11** hotels
- Reservation databases were hacked by cyberattack
- Approximately **1.2 million** affected
- Personal data involved: name, date of birth, address, phone number, HKID and passport number (even payment information in a small number of cases)

## Hong Kong Technology Venture Company Limited

- The operator of a popular e-commerce platform **HKTVMall**
- “A small portion” of the 4.38 million registered customer information was accessed
- Personal data involved: name, delivery address, phone number, email address, etc.

# PCPD to follow up on Data Breaches

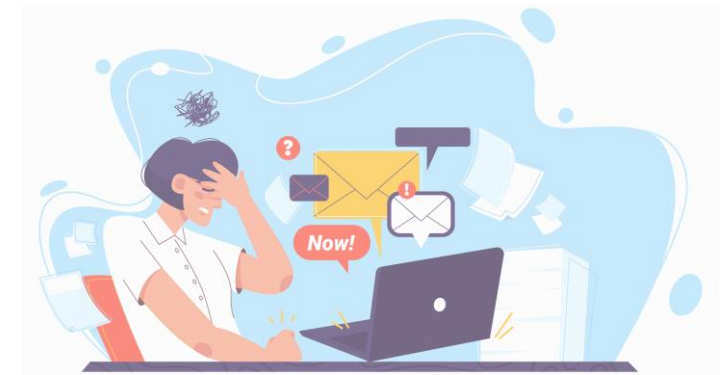
Organisations may sacrifice their **goodwill**, as well as the **trust** of their customers in the event of a data breach incident

Reporting the incident to the PCPD

The PCPD may give advice on the handling of data breaches



**NOTE:** The PCPD may commence an investigation into the incident **whether a report is made or not**





# 6 Data Protection Principles (DPPs)

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。

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

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。

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.

收集的資料是有實際需要的，而不超乎適度。

Data collected should be necessary but not excessive.

2

## 準確性、儲存及保留 Accuracy & Retention



資料使用者須採取切實可行的步驟以確保持有的個人資料準確無誤，而資料的保留時間不應超過達致原來目的實際所需。

Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil 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 practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

5

## 透明度 Openness



資料使用者須採取切實可行的步驟來公開其處理個人資料的政策和行事方式，並交代其持有的個人資料類別和用途。

A data user must take practicable steps to make personal data policies and practices known to the public regarding the 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.

# Data Privacy Pitfalls

## Potential Criminal Liability

## PDPO Criminal Offences (non-exhaustive)

### Enforcement Notice

1. Contravention of an enforcement notice (**S.50A**)



### Direct Marketing

#### PART 6A

1. Data user must not use personal data in direct marketing without data subject's consent (**S.35E**)
2. Data user must notify data subject when using personal data in direct marketing for first time (**S.35F**)
3. Data user must comply with data subject's requirement to cease to use personal data in direct marketing (**S.35G**)

### Doxxing

1. Disclosing personal data without data subject's consent (**S.64(3A)** and **64(3C)**)
  - a) with an intent to cause any specified harm to the data subject or his/her family member
  - b) being reckless as to whether any specified harm would be caused

### Others

1. Failure to erase personal data no longer required (i.e. prolonged retention of personal data) (**S.26**)
2. Obstructing, hindering or resisting the Privacy Commissioner in performing her functions or exercising her powers (**S.50B(1)**)



# Data Privacy Pitfalls

## PDPO Criminal Offences – Case Sharing: Direct Marketing

**Telecommunications Company  
Pleaded Guilty to Violating  
Direct Marketing Provisions and  
Fined HK\$12,000**



### Using Personal Data in Direct Marketing

#### **Background:**

A complainant had subscribed broadband service with a telecommunications company and opted out the use of his personal data in direct marketing. However, the complainant still received three direct marketing calls promoting a new service plan.

The complainant complained to the PCPD. The case was subsequently referred to the Police for follow-up actions. In 2020, the telecommunications company pleaded guilty to six charges and was fined \$12,000.

#### **Takeaway:**

- ✓ Organisations should not ignore customers' opt-out requests.
- ✓ Developing and implementing policies, as well as providing proper training to employees, are important

# Data Privacy Pitfalls

## IN MOST CASES...

The data user (*a company*) that contravenes requirements under the PDPO is a body corporate.

- Separating “**corporate legal entity**” and “**people running the company**” (directors)

**Telecommunications Company** Pleaded Guilty to Violating Direct Marketing Provisions and Fined HK\$12,000

Direct marketing offence admitted:  
**Auction company** fined HK\$20,000



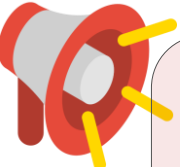
# Data Privacy Pitfalls

## a) Potential Criminal Liability

### CRIMINAL PROCEDURES ORDINANCE (Cap. 221)

#### Section 101E Liability of directors, etc.:

Where a person by whom an offence has been committed is a company and it is proved that the offence was committed with the consent or connivance of a director, the director shall be guilty of the like offence.



If a company (as data user) is found to have committed a criminal offence under the PDPO, a director may also be held criminally liable for such offence (if it is proved that the offence was committed with the consent or connivance of the director).



# Data Privacy Pitfalls

## b) Potential Civil Liability

### PERSONAL DATA (PRIVACY) ORDINANCE (Cap. 486) (PDPO)

#### Section 65 Liability of employers:

(1): Any act done by a person in the course of his employment shall be treated as done by his employer as well, whether or not it was with the employer's knowledge or approval.

(3): In proceedings brought under PDPO against any person in respect of an act alleged to have been done by an employee, it shall be a defence for that person to prove that he took practical steps to prevent the employee from doing that act.



# Data Privacy Pitfalls

## c) Other Regulatory Liability

### SECURITIES AND FUTURES ORDINANCE (Cap. 571)

#### Section 307B Requirement for listed corporations to disclose inside information:

A listed corporation must, as soon as reasonably practicable after any inside information has come to its knowledge, disclose the information to the public.

**Inside information:** *“likely to materially affect the price of the listed securities”*

Similar disclosure obligations can also be found under the Listing Rule (Rule 13.09)



*Hong Kong Technology Venture Company Limited made a voluntary announcement to follow up on the HKTVMall data breach*



# Data Privacy Tips for Directors

# Data Privacy Tips

## a) Data Governance

## PERSONAL DATA PRIVACY MANAGEMENT PROGRAMME (PMP)

### BACKGROUND

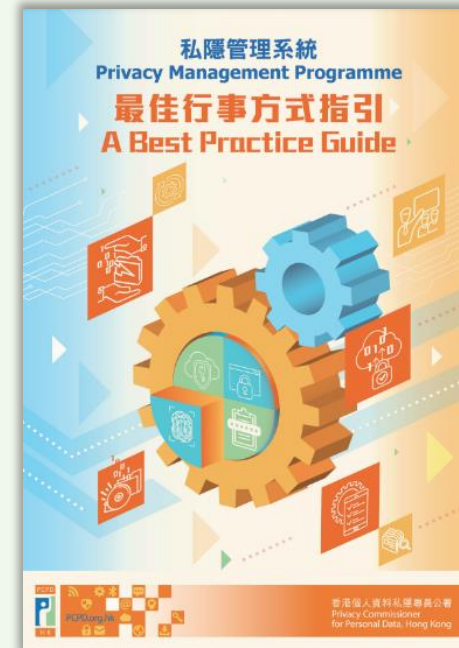
#### The PMP Guide:

- Recommends organisations to embrace personal data protection as part of their corporate policies and culture

#### Benefits:

- Minimising the risk of data security incidents
- Effective handling of data breaches to minimise damage
- Ensuring compliance with the PDPO
- Demonstrating the organisation's commitment

### *Personal Data Privacy Management Programme: A Best Practice Guide*



# Data Privacy Tips

## a) Data Governance

## PERSONAL DATA PRIVACY MANAGEMENT PROGRAMME

### CONTENT

#### 1. Organisational Commitment

- Buy-in from the Top
- Appointment of Data Protection Officer
- Establishment of Reporting Mechanisms

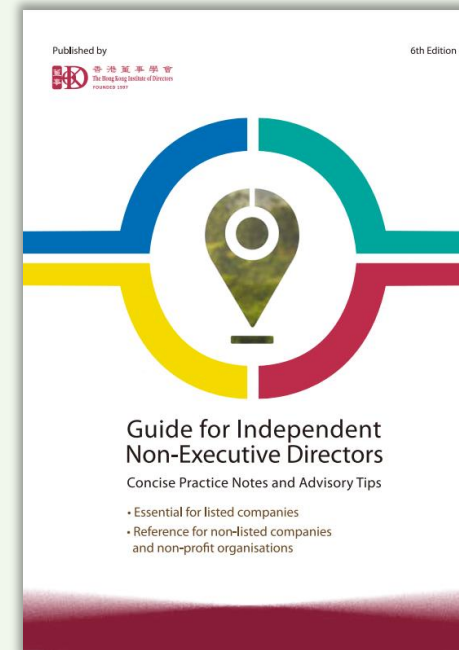
#### 2. Programme Controls

#### 3. Ongoing Assessment and Revision

ESG

Implementation of PMP is also recommended in “*Guide for Independent Non-Executive Directors*” published by HKIoD

### *HKIoD: Guide for Independent Non-Executive Directors*



# Data Privacy Tips

## a) Data Governance

## PERSONAL DATA PRIVACY MANAGEMENT PROGRAMME



### 2. Programme Controls

2.1 Personal Data Inventory

2.2 Internal Policies on Personal Data Handling

2.3 Risk Assessment Tools

2.4 Training, Education and Promotion

2.5 Handling of Data Breach Incident

2.6 Data Processor Management

2.7 Communication

# Data Privacy Tips

## a) Data Governance

## DATA SECURITY

*Guidance Note on Data Security Measures for Information and Communications Technology*

**COMING SOON!**

### CONTENT

**Directors may pay attention to:**

- *Data governance and organisational measures (policy & procedures) (Part C(1))*
- *Data Processor management (Part C(4))*
- *Monitoring, evaluation and improvement (Part C(6))*

HKCERT



The guidance incorporated comments of **Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT)**

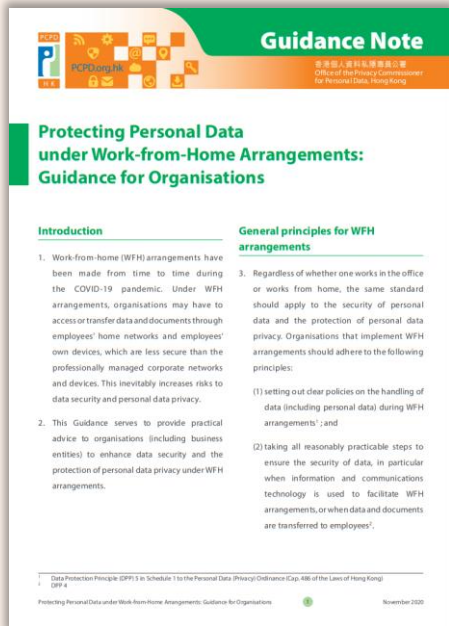


# Data Privacy Tips

## b) Other Practical Tips

## WORK-FROM-HOME ARRANGEMENTS

### Protecting Personal Data under Work-from-Home Arrangements: Guidance for Organisations



### BACKGROUND

- Organisations have to access or transfer data, including personal data, under work-from-home (WFH) arrangements

### The Guidance:

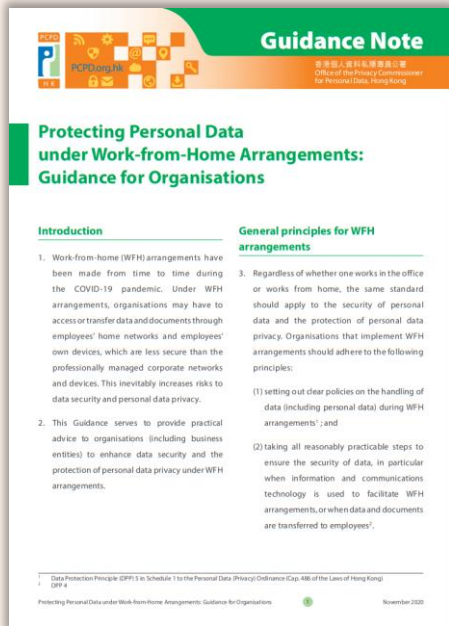
- Provides practical advice to organisations to enhance data security and privacy protection in the context of WFH

# Data Privacy Tips

## b) Other Practical Tips

## WORK-FROM-HOME ARRANGEMENTS (cont'd)

### Protecting Personal Data under Work-from-Home Arrangements: Guidance for Organisations



### CONTENT

The practical advice covers the following areas:

- *Policies and guidance*
- *Staff training and support*
- *Device management*
- *Virtual Private Network & remote access management*



Under this series, PCPD also issued practical guidance notes for **employees** and **video conferencing software users**

# Data Privacy Tips

## b) Other Practical Tips

## EMPLOYEES' PERSONAL DATA (COVID-19)

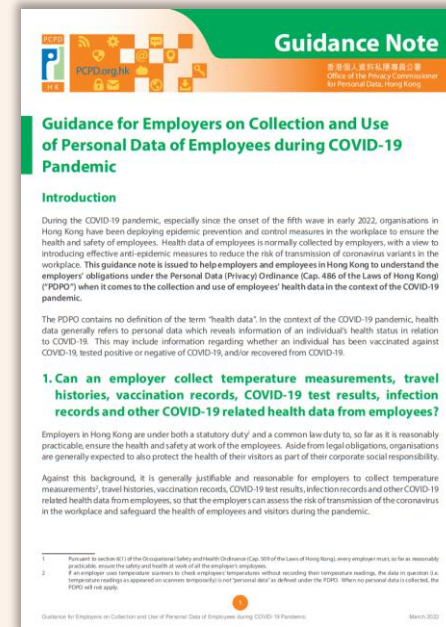
### BACKGROUND

- During the COVID-19 pandemic, organisations often deploy epidemic prevention and control measures in the workplace
- Employers have been collecting health data of employees, e.g. vaccination status, COVID-19 test results

### The Guidance:

- Provides Q&As to help employers and employees understand what can and cannot be done

### Guidance for Employers on Collection and Use of Personal Data of Employees during COVID-19 Pandemic



# Data Privacy Tips

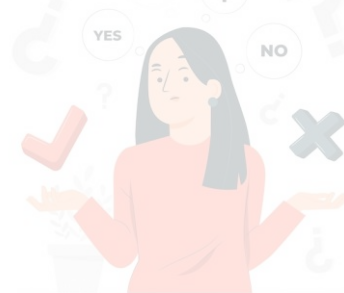
## b) Other Practical Tips

## EMPLOYEES' PERSONAL DATA (COVID-19) (cont'd)

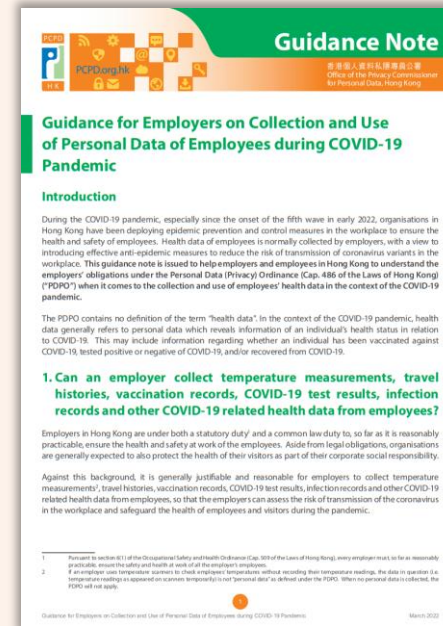
### EXAMPLES

**Q.1:** Can an employer collect COVID-19 related health data from employees?

**Q.2:** Can an employer collect the health data of an employee's family member(s)?



### Guidance for Employers on Collection and Use of Personal Data of Employees during COVID-19 Pandemic





# Contact Us

The screenshot shows the PCPD website homepage. At the top, there is a header with the PCPD logo, the website URL 'PCPD.org.hk', and the name in Chinese '香港個人資料私隱專員公署' and English 'Office of the Privacy Commissioner for Personal Data, Hong Kong'. Below the header is a banner with the slogan '保障、尊重個人資料私隱' and 'Protect, Respect Personal Data Privacy'. A navigation menu includes links for 'About PCPD', 'Data Privacy Law', 'News & Events', 'Enforcement Reports', 'Frequently Asked Questions', 'Compliance & Enforcement', and 'Doxxing Offences NEW!'. There are also links for 'Complaints', 'Education & Training', 'Resources Centre', and 'Contact Us'. A search bar with 'Hot Search' and 'Advanced Search' options is present. Below the search bar are social media icons for Facebook, Instagram, LinkedIn, Twitter, Weibo, and YouTube. The main content area features a 'What's New' section with several news items, including 'PCPD Releases Report on "Comparison of Privacy Settings of Social Media"', 'Privacy Commissioner's Office Broadcasts TV Video and Radio Announcement on Doxxing Offences', and 'Privacy Commissioner Published an Article on "New Recommended Model Clauses for Cross-border Transfer of Personal Data"'. At the bottom of the page, there are buttons for 'For Individuals' and 'For Organisations'.

- ☐ Hotline 2827 2827
- ☐ Fax 2877 7026
- ☐ Website [www.pcpd.org.hk](http://www.pcpd.org.hk)
- ☐ E-mail [communications@pcpd.org.hk](mailto:communications@pcpd.org.hk)



спасибо  
danke 謝謝  
ngiyabonga  
teşekkür ederim  
dank je  
gracias  
tapadh leat  
bedankt  
huala  
maururu  
thank you  
mochchakkeram  
dziękuję  
sagolun  
sukriya  
kop khun krap  
go raibh maith agat  
arigatō  
takk  
dakujem  
merci  
obrigado  
terima kasih  
ευχαριστώ  
감사합니다