

Webinar on the Protection of Personal Data Privacy for NGOs

The Hong Kong Council of Social Service

8 November 2021



Mr Anthony CHAN
Senior Personal Data Officer (Complaints)



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



守護 · 私隱 · 廿五載
GUARDIAN · PRIVACY · 25 YEARS

Focus of the talk

- Exemptions of the Ordinance, e.g. Section 58
- Handling of data breach
- Proper way of conducting direct marketing & privacy impact assessment

Privacy right is **not absolute**

Basic Law of HKSAR, PRC

- Article 30: “... **No** department or individual may, on any grounds, **infringe** upon the freedom and privacy of communication of residents **except** that the relevant authorities may inspect communication **in accordance with legal procedures to meet the needs of public security** or of investigation into criminal offences.”

Hong Kong Bill of Right Ordinance (BORO)

- Section 5: “In time of **public emergency** which threatens the life of the nation and the existence of which is officially proclaimed, measures may be taken **derogating** from the Bill of Rights **to the extent strictly required** by the exigencies of the situation, but these measures shall be **taken in accordance with law**.”

Personal Data (Privacy) Ordinance (PDPO)

- Part 8: Exemptions, e.g.
 - Exempted from use limitation (i.e. DPP 3) if application of DPP 3 would be likely to **prejudice** the specified purposes, such as
 - Section 57: **Security** of Hong Kong
 - Section 58: Prevention or detection of **crimes**, etc.
 - Section 60B: **Legal proceedings**



Exemptions

Section 58 – Crimes, etc.



- Examples under section 58(1) :
 - Prevention or detection of crime (section 58(1)(a))
 - Apprehension, prosecution or detention of offenders (section 58(1)(b))
 - Prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty (section 58(1)(d))
- To satisfy the prejudice Test (section 58(2)):
 - Whether disclosure of the personal data would likely prejudice the above purpose
- Confine to offence under the laws of Hong Kong
- Exempt from compliance with DPP 3 (use) and DPP 6 (access request)

Exemptions



- **Seriously Improper Conduct**
 - Breach of a tortious duty for failure to maintain a canopy in a safe condition (Lily Tse Lai Yin & Ors v The Incorporated Owners of Albert House & Others [1999] 1 HKC 386) ✓
 - Serious indebtedness of an officer of a law enforcement agency (AAB No.5/2006) X
 - Failure to honour a cheque, without evidence of fraud or dishonesty (AAB No.14/2004) X

Exemptions



Section 58 – Crimes, etc.

- **Practical Tips**

- How to respond to an enquiry from a law enforcement agency for personal data of your customer / client?
 - Assess whether there are reasonable grounds for believing, at the material time, that **non-provision** of the requested material **would be likely to prejudice the purpose** (e.g. for detection or prevention of crime or seriously improper conduct).
 - determine from **all circumstances of the case** (such as the nature of the material so requested) whether there is any other channel where such material could be obtained, etc.

Exemptions



Section 58 – Crimes, etc.

- Before data user invokes the exemption, it would be prudent for the data user to make further enquiries to the requestor as to:
 - 1) the **purpose** for which the personal data is to be used
 - 2) the reason why the personal data concerned is **relevant to or necessary** for the purpose
 - 3) the reason why the **data subject's consent** is not obtained by the agency
 - 4) whether the personal data can be obtained from **other source**;
 - 5) in particular, how the application of DPP3 would be likely to **prejudice the purpose**

Exemptions



Section 59 – Public health

- Personal data relating to the physical or mental health of the data subject is exempt from the application of DPP6 / DPP3
- If such application would be **likely to cause serious harm** to the physical or mental health of:
 - the data subject; or
 - any other individual
- Disclosure of patient's condition to employer without patient's consent
(AAB No.15/2009) ✓



Exemptions

Section 60B – Legal Proceedings

Disclosure authorised by law

- DPP3 is exempted if use of data is **required or authorised by law or court order in Hong Kong (section 60B(a))**

Legal proceedings, etc.

- DPP3 is exempted if use of data is:
 - Required in connection with legal proceedings in Hong Kong (**section 60B(b)**) (i.e. where proceedings have been **commenced**)
 - Required for establishing, exercising or defending legal rights in Hong Kong (**section 60B(c)**) (i.e. where proceedings are **contemplated**)

DPP 1:
collection
purpose &
means

DPP 2:
accuracy &
retention

DPP 3: use

DPP 4:
security

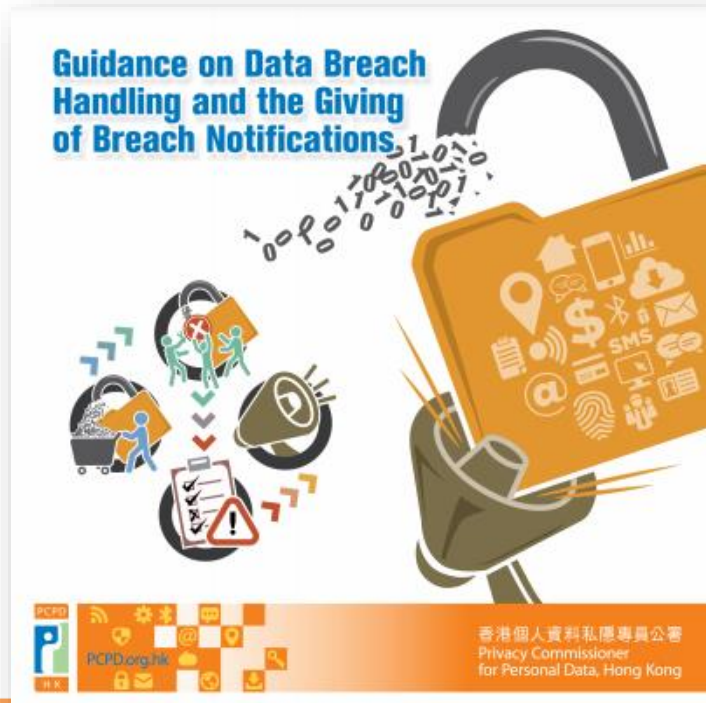
DPP 5:
Openness

DPP 6: data
access &
correction

How to handle a data breach?

1. What is a data breach?

- A suspected breach of data security of personal data held by a data user
- Exposing the data to the risk of unauthorized or accidental access, processing, erasure, loss or use
- May amount to contravention of DPP 4

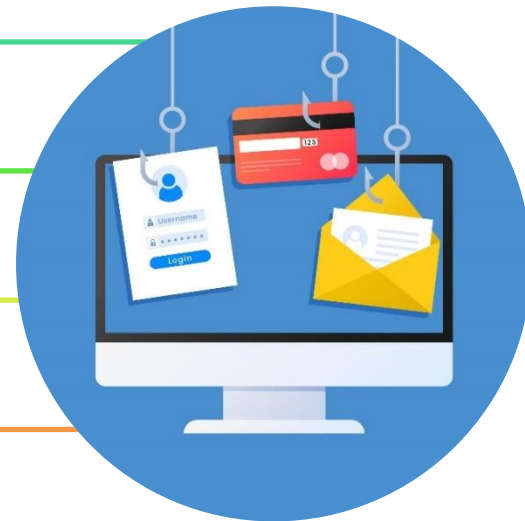


Requirement of DPP4

- all practicable steps shall be taken to ensure that personal data are protected against **unauthorized or accidental access, processing, erasure, loss and use**
- security in the storage, processing and transmission of data
- if a data user engages a data processor to process personal data on the data user's behalf, the data user must adopt **contractual or other means** to prevent unauthorized or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing

Common types of data breach

1. Loss of documents and USB
2. Improper setting of IT system or Hacking
3. Wrong (e)mailing address
4. Staff's integrity and prudence
5. Improper disposal of documents



How to handle a data breach?

2. What should be done?

Collecting information immediately

When? Where? How? How many?
What (cause + kinds of personal data involved)

Contacting the interested parties

Police? Internet companies? IT experts?

Adopting containment measures

Stop the system? Change password? Technical assistance? Keeping evidence? Data processors?

Assessing the harm

Personal safety? Identity theft? Financial loss?
Damage to reputation?

Considering the giving of notification

Real risk of harm is reasonably foreseeable
Notify data subjects? **Notify PCPD?**

DPP 1:
collection
purpose &
means

DPP 2:
accuracy &
retention

DPP 3: use

DPP 4:
security

DPP 5:
Openness

DPP 6: data
access &
correction



PCPD.org.hk

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



Give data breach notification to PCPD?

- NOT a statutory requirement
- A recommended practice

How?

- Download the “Data Breach Notification Form” from PCPD’s website
- Submit the completed form to PCPD by fax, in person, by fax or by post

Data Breach Notification Form

Notice

Notification of a data breach to the Privacy Commissioner for Personal Data, Hong Kong (the “Commissioner”) by the data user (see Note 1) is not a legal requirement. In deciding whether or not to give this notification to the Commissioner, you should consider the “Guidance on Data Breach Handling and the Giving of Breach Notifications” issued by the Commissioner. In most cases, it is advisable to give notification to the data subject(s) (see Note 2) affected by the breach.

PARTICULARS OF THE PERSON GIVING THIS NOTIFICATION (i.e. the data user)

Name: _____
Address: _____
Telephone number: _____ Fax number: _____
Email address: _____

Where the person giving this notification is an organization, please provide the following information:

Contact person: _____
Name (“Mr./Ms./Mrs.”): _____
Relationship with the Reporting Organization (e.g. job title): _____
Telephone number: _____ Fax number: _____
Email address: _____
(*Please delete as appropriate)

DETAILS ABOUT THE DATA BREACH (see Note 3):

About PCPD | Data Privacy Law | News & Events | Enforcement Reports | Frequently Asked Questions | Compliance & Enforcement | Complaints |
Education & Training | Resources Centre | Contact Us

Home > Compliance & Enforcement > Data Breach Notification

Compliance & Enforcement

- Court Judgment
- Administrative Appeals
- Board's Decisions
- Case Notes
- Data Breach Notification
- Submissions on Privacy Issues
- Consultations

Data Breach Notification

A data breach is generally taken to be a suspected breach of data security of personal data held by a data user, by exposing the data to the risk of unauthorised or accidental access, processing, erasure, loss or use.

While it is not a statutory requirement on data users to inform the PCPD about a data breach incident concerning the personal data held by them, data users are nevertheless advised to do so as a recommended practice for proper handling of such incident. You may make reference to our “[Guidance on Data Breach Handling and the Giving of Breach Notifications](#)” before submitting a data breach notification.

For submitting a data breach notification to the PCPD, please click here to download the Data Breach Notification Form. You can then fill in the form by making reference to the “Notice” and “Information Notes” contained therein.

After completing the form, please submit it and other relevant documents concerning the data breach (if any) which you wish to provide by the following channels:-

- By Post / In Person
Address:
Room 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai Hong Kong

Opening hours of Reception Counter:
Monday to Friday: 8:45 a.m. to 12:45 p.m. & 1:50 p.m. to 5:40 p.m.

• By Fax
Fax number: 2877 7026
- By Email
Email address: dbn@pcpd.org.hk

Data Breach Notification

- it is **not a statutory requirement** on data users to inform the PCPD about a data breach incident concerning the personal data held by them, but data users are advised to do so as a recommended practice for proper handling of such incident.



Data Breach Handling



Collecting Information Immediately

Immediate gathering of essential information for assessing the impact on data subjects including:

- When and where did the breach take place?
- How was the breach detected and by whom?
- What was the cause of the breach?
- What kind and extent of personal data was involved?
- How many data subjects were affected?

Data Breach Handling



Action

Contacting the Interested Parties & Adopting Containment Measures

Interested parties may include:

- The law enforcement agencies
- The relevant regulators (e.g. Privacy Commissioner for Personal Data, Hong Kong (the “Commissioner”))
- The Internet companies
- IT experts

17

PCPD



H K

PCPD.org.hk

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



Data Breach Handling



Assessing the Harm

Assessing the potential harm caused by a data breach, for examples:

- Threat to personal safety
- Identity theft
- Financial loss
- Humiliation or loss of dignity, damage to reputation or relationship
- Loss of business and employment opportunities

18

Data Breach Handling



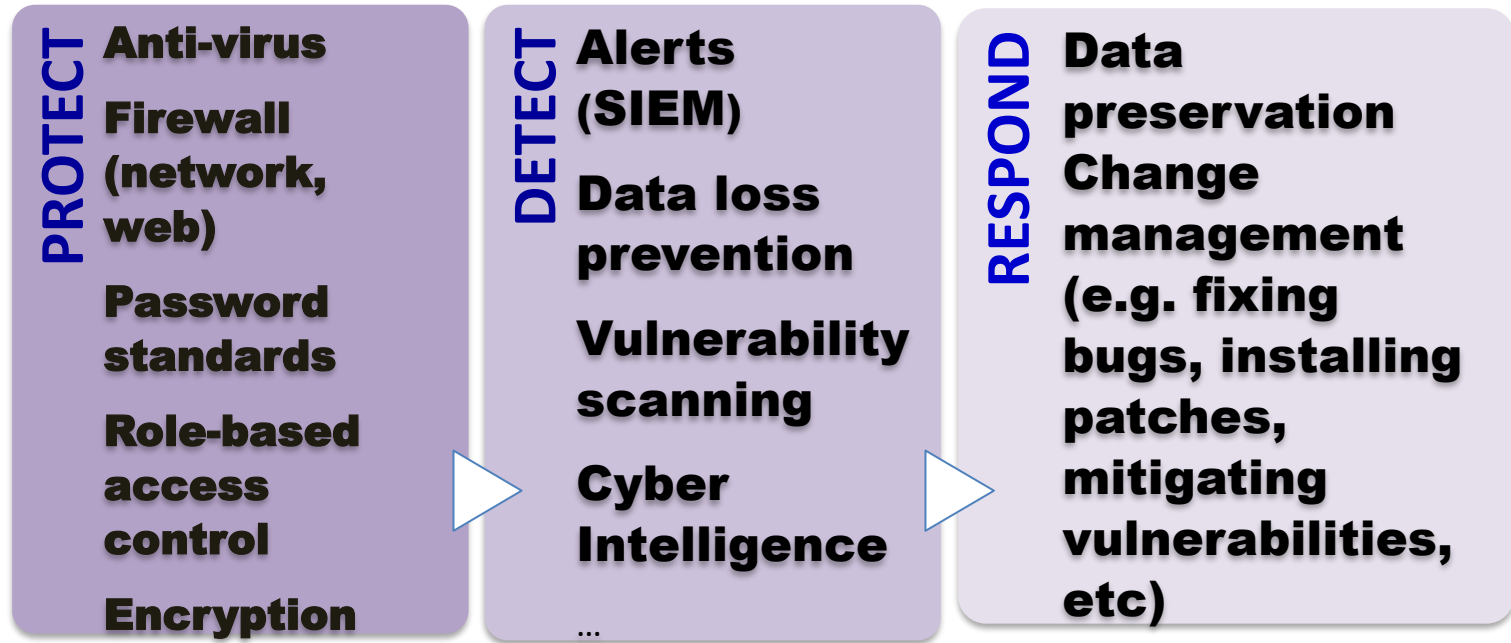
Considering the Giving of Notification

When real risk of harm is reasonably foreseeable in a data breach, the data user should consider:

- Notifying the affected data subjects and the relevant parties
- The consequences for failing to give notification

Security of Personal Data

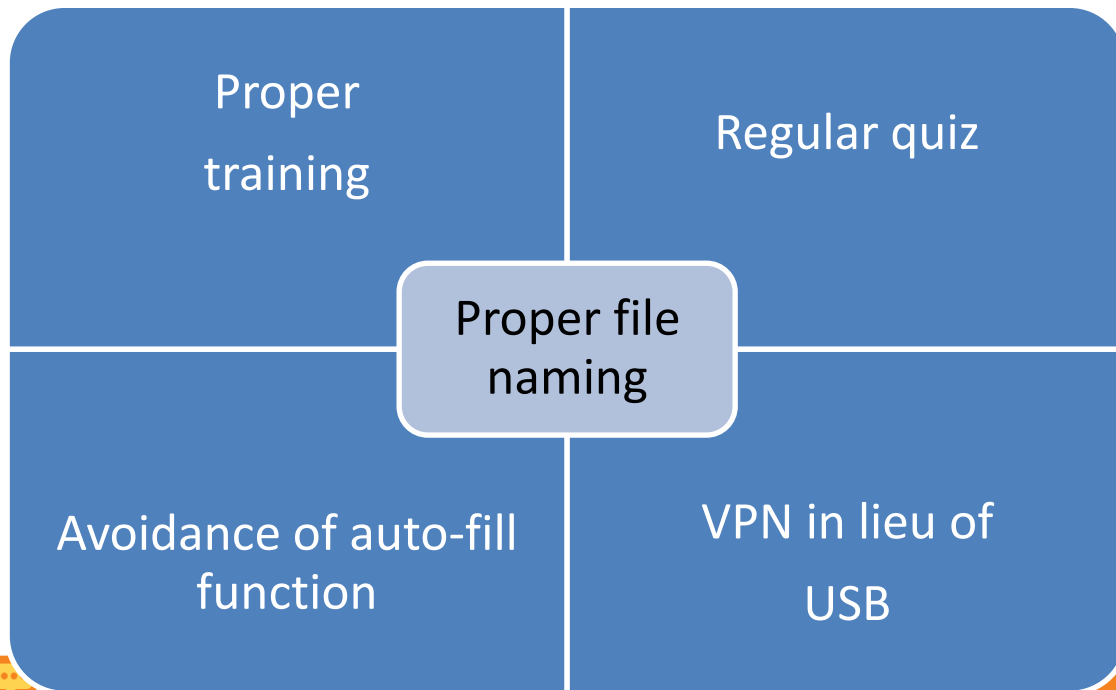
Technical security measures



20

Security of Personal Data

How to avoid human errors



PCPD



H K

PCPD.org.hk

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



守護 · 私隱 · 廿五載
GUARDIAN · PRIVACY · 25 YEARS

Direct Marketing Regulatory Regime

Part 6A of the PDPO:
section 35A to section 35M
(to replace the original section 34)

Effective on 1 April 2013

22

New Guidance on Direct Marketing

Exercising Your Right of Consent to and Opt-out from Direct Marketing Activities under the Personal Data (Privacy) Ordinance¹

It is common for members of the public to receive unsolicited telephone calls, mail, email, messages and so on from direct marketers promoting various products and services.

Under the Personal Data (Privacy) Ordinance ("the Ordinance"), organisations are required to notify you and obtain your consent before using your personal data in their own direct marketing activities or transferring the data to another person for use in the latter's direct marketing activities.

Despite your consent to use your personal data in direct marketing, direct marketers must notify you of your opt-out right when using your personal data in this manner for the first time. On the other hand, you may require them to cease to use the data at any time. The request must be complied with at no cost to you. Further, despite your consent for an organisation to transfer your personal data to third parties for use in the latter's direct marketing activities, you may at any time require the organisation to cease to transfer the data and to notify any person to whom your personal data has been so transferred to cease to use the data in direct marketing. Again the request must be complied with at no cost to you.

For contraventions of the requirements under the Ordinance involving the transfer of personal data to third parties for gain, the maximum penalty is a fine of HK\$1,000,000 and imprisonment for 5 years. For other direct marketing contraventions, the maximum penalty is a fine of HK\$500,000 and imprisonment for 3 years.

The purpose of this leaflet is to explain the direct marketers' obligations when using your personal data and how you may exercise your right to indicate your consent to the intended use or transfer of your personal data in direct marketing. It also guides you to make an opt-out request under the Ordinance in order to effectively stop an organisation from continuing to use or transfer your personal data for direct marketing purposes.

▶ Q1 What is "direct marketing"?

Under the Ordinance, "direct marketing" means:

- (a) the offering, or advertising of the availability, of goods, facilities or services; or
- (b) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes

by the following direct marketing means:

- (i) sending information or goods, addressed to specific persons by name by mail, fax, electronic mail or other means of communication; or
- (ii) making telephone calls to specific persons.

Hence direct marketing under the Ordinance does not include unsolicited business electronic messages² without addressing to specific persons by name and person-to-person calls being made to phone numbers randomly generated.

¹ This leaflet takes effect on 1 April 2013; the date of commencement of the new provisions of the Ordinance. It updates and replaces the leaflet on this subject issued in November 2011.

² Please refer to the Unsolicited Electronic Messages Ordinance (Cap. 593) enforced by the Office of the Communications Authority.

Guidance Note

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

New Guidance on Direct Marketing

PART 1: Introduction

Purpose of guidance

1.1 Direct marketing is a common business practice in Hong Kong. It often involves collection and use of personal data by an organization for direct marketing itself and in some cases, the provision of such data by the organization to another person for use in direct marketing. In the process, compliance with the requirements under the Personal Data (Privacy) Ordinance (the "Ordinance") is essential. This document is issued by the Privacy Commissioner for Personal Data (the "Commissioner") to provide practical guidance on data users' compliance with the new regulatory requirements for direct marketing under the new Part VIA of the Ordinance¹. It helps data users to fully understand their obligations as well as to promote good practice. Data users should also make reference to other laws, regulations, guidelines and codes of practice that are relevant for direct marketing purposes insofar as they are not inconsistent with the requirements under the Ordinance.

1.2 This Guidance shall take effect on the same date as the date of commencement of Part VIA of the Ordinance (the "commencement date"). It will supersede and replace the Commissioner's "Guidance on the Collection and Use of Personal Data in Direct Marketing" issued in November 2012. For the avoidance of doubt, until Part VIA of the Ordinance

takes effect, the Commissioner's "Guidance on the Collection and Use of Personal Data in Direct Marketing" remains fully valid.

What is "direct marketing"?

1.3 The Ordinance does not regulate all types of direct marketing activities. It defines "direct marketing" as:

- (a) the offering, or advertising of the availability, of goods, facilities or services; or
 - (b) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes,
- through **direct marketing means**².

"Direct marketing means" is further defined to mean:

- (a) sending information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or
- (b) making telephone calls to specific persons.

1.4 Hence, "direct marketing" under the Ordinance does not include unsolicited business electronic messages sent to telephones, fax machines or email addresses without addressing to specific persons by name and person-to-person calls being made to phone numbers randomly generated.

¹ The new Part VIA under the Ordinance was introduced by the Personal Data (Privacy) (Amendment) Ordinance 2012. It will take effect on 1 April 2013.

² Section 35A(1).

³ Please refer to the Unsolicited Electronic Messages Ordinance (Cap. 593, Laws of Hong Kong) enforced by the Office of the Communications Authority.

New Guidance on Direct Marketing

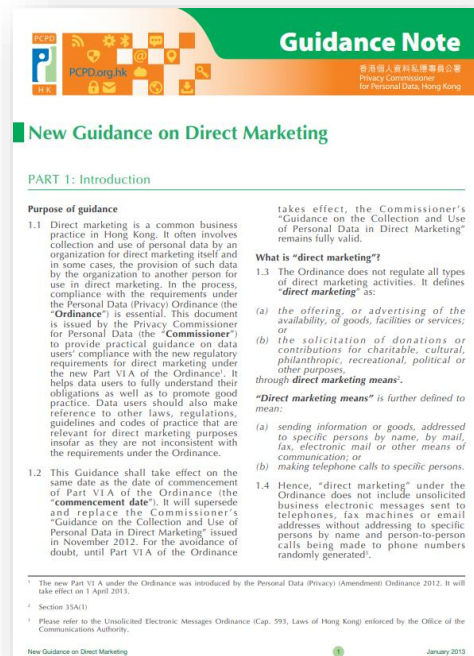
Part 1: Introduction

Part 2: **Collection** of personal data for direct marketing

Part 3: **Use** of personal data in direct marketing

Part 4: **Providing** personal data to another person for use in direct marketing

Part 5: Other practical guidance relating to direct marketing



What is “Direct Marketing”?

“**Direct marketing**” is defined to mean:

- a. the **offering**, or advertising of the **availability**, of goods, facilities or services; or
- b. the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes, through **direct marketing means** (Section 35A(1)).



“**Direct marketing means**” is further defined to mean:

- a. sending information or goods, **addressed to specific persons by name**, by mail, fax, electronic mail or other means of communication; or
- b. making telephone calls to **specific persons**.

25

PCPD



H K

PCPD.org.hk

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



守護 · 私隱 · 廿五載
GUARDIAN · PRIVACY · 25 YEARS

Regulated by PDPO ?



26

PCPD



H K



PCPD.org.hk

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



Examples of DM

- A telecommunications service provider approaches its existing customers by telephone to offer upgraded services
- A beauty salon offers a free beauty treatment by telephone to a specific person

Examples: ~~X~~ DM under the PDPO

- A service provider sends an SMS to its existing customers **informing** them of **the impending expiration** of their service contracts and providing an enquiry hotline
- **Direct mail** sent to an address or the “occupant” of an address **without addressing specific persons** by name
- A customer service manager introduces goods/services to a customer **face-to-face**



28

Examples: ~~✗~~ DM under the PDPO

- A tutorial centre creates a WhatsApp group, adds a massive list of mobile phone numbers with the same prefix (without knowing other personal data of the number owners) into the group and then sends messages to group members promoting its referral services



29

Use of personal data in direct marketing

Steps a data user must take :

1. Inform the data subject (s.35C (2)(a))-
 - Data user **intends** to so use the personal data
 - Data user may not so use the data unless the data subject **consents** to it
2. Provide the data subject with the following information (s.35C (2)(b))--
 - The **kinds** of personal data to be used
 - The **classes** of marketing subjects
 - A **channel** through which the data subject may communicate his consent to the intended use
3. Receive consent from data subject -
 - In writing (s. 35E(1)(a))
 - Consent given orally (s. 35E(1)(b))

30

Providing personal data to third parties for direct marketing


Steps a data user must take :

1. Inform the data subject in writing (s.35J(2)(a))-
 - Data user **intends** to so provide the personal data
 - Data user may not so provide the data unless he receives **written consent**
2. Provide the data subject with the following information (s.35J (2)(b))—
 - If the data is to be provided **for gain**, that the data is to be so provided
 - The **kinds** of personal data to be used
 - The **classes** of marketing subjects
 - A **channel** through which the data subject may communicate his consent to the intended use
3. **Receive written consent** from data subject

31

Rights of the data subjects

1. Request data user to cease to use the data in direct marketing (s.35G(1))
2. Request data user (s.35L(1)) –
 - to **cease to provide** his personal data to any other person for use by that other person in direct marketing
 - to **notify** that other person to cease to use the data in direct marketing



Data users must comply with the requests **without charge to the data subject**

32

Criminal penalties

Offence	Relevant section	Maximum Fine (HK\$)	Maximum Imprisonment
Subject to section 35D, a data user who uses a data subject's personal data in direct marketing but fails to take any of the following actions:- (1) inform the data subject:- (a) the data user intends to so use the personal data; (b) the data user may not so use the data unless with the data subject's consent; (c) the kinds of personal data to be used; (d) the classes of marketing subjects which the data is to be used; (2) provide the data subject with a response channel through which the data subject may, without charge, communicate his consent to the intended use.	35C(5)	\$500,000	3 years
A data user who uses a data subject's personal data in direct marketing without observing any of the following:- (1) having received the data subject's consent to the intended use; (2) having sent a written confirmation to the data subject within 14 days from receiving the consent if given orally, confirming:- (a) the date of receipt of the consent; (b) the permitted kind of personal data; and (c) the permitted class of marketing subjects. (3) the use of the personal data is consistent with the data subject's consent.	35E(4)	\$500,000	3 years
A data user who, when using a data subject's personal data in direct marketing for the first time, fails to inform the data subject that the data user must, without charge, cease to use the data in direct marketing if the data subject so requires.	35F(3)	\$500,000	3 years
A data user who fails to comply with the request to cease to use personal data in direct marketing made by a data subject without charge.	35G(4)	\$500,000	3 years

Offence	Relevant section	Maximum Fine (HK\$)	Maximum Imprisonment
A data user who fails to take any of the following actions before providing personal data to another person for use in direct marketing:- (1) inform the data subject in writing:- (a) the data user intends to so provide the personal data; (b) the data user may not so provide the data unless with the data subject's written consent; (2) provide the data subject with written information in relation to:- (a) where the data is to be provided for gain, that the data is to be so provided; (b) the kinds of personal data to be provided; (c) the classes of persons to which the data is to be provided; (d) the classes of marketing subjects which the data is to be used; (3) provide the data subject with a response channel through which the data subject may, without charge, communicate his consent to the intended use.	35J(5)	\$1,000,000 (for gain) \$500,000 (not for gain)	5 years (for gain) 3 years (not for gain)
A data user who provides the data subject's personal data to another person for use in direct marketing without observing any of the following:- (1) having received the data subject's written consent to the intended provision of personal data; (2) if the data is provided for gain, having specified in the information provided to the data subject the intention to so provide; (3) the provision of the data is consistent with the data subject's consent.	35K(4)	\$1,000,000 (for gain) \$500,000 (not for gain)	5 years (for gain) 3 years (not for gain)
A data user who fails to comply with a data subject's request to:- (1) cease to provide the data subject's personal data for use in direct marketing; or (2) notify any data transferee in writing to cease to use the data in direct marketing.	35L(6)	\$1,000,000 (for gain) \$500,000 (in any other case)	5 years (for gain) 3 years (in any other case)
A data transferee who fails to comply with a data user's written notification to cease to use a data subject's personal data in direct marketing	35L(7)	\$500,000	3 years

熱門話題：修政議事制度、習近平博覽講話、連德豪、Tesla致命車禍、許樹昌、麗城花園、歐洲超級聯賽、河引(圖輯)

港聞 [客戶拒收直銷信息仍接保險推廣 花旗被控違私隱條例罰款1萬]

2019年5月21日 星期二

客戶拒收直銷信息仍接保險推廣 花旗被控違私隱條例罰款1萬 (18:46)

📱 📧 📞 📺 📷 📹 📻 📡 📢 📣 📤 📥 📦 📧 📨 📩 📪 📫 📬 📭 📮 📯 📰 📱 📲 📳 📴 📵 📶 📷 📸 📹 📺 📻 📼 📽 📾 📿



圖1-花旗銀行位於維多利亞道(即「金鐘」)第355號。今……(資料圖片)



香港個人資料私隱專員公署2016年接獲投訴，投訴人於2016年8月透過互聯網申請花旗銀行信用卡時，選擇拒收直接促銷資訊，惟同年10月卻收到該銀行推廣保險服務的來電。花旗銀行被控違反《個人資料(私隱)條例》第35(3)條，今日(21日)在九龍城裁判法院承認控罪，被判罰款1萬元。



PCPD.org.hk

Convictions

Media Statements

Date: 12 September 2019

Direct Marketing Offence Admitted: Telecommunications Company Fined HK\$84,000

SmarTone Mobile Communications Limited (SmarTone) faced 23 charges under the Personal Data (Privacy) Ordinance (the Ordinance) today at the Kwan Tong Magistrates' Courts. All charges related to the offence of failing to comply with the requirement from the data subject to cease to use her personal data in direct marketing, contrary to section 35(3) of the Ordinance. The Company pleaded guilty to 14 charges, and was fined HK\$84,000 in total (HK\$6,000 in respect of each charge). This single case has recorded the highest number of charges and the second highest amount of fine since the added provisions of the Ordinance relating to regulating direct marketing activities came into effect on 1 April 2013.

Case Background

The case stemmed from a complaint received by the office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD) in 2017. The complainant received 23 direct marketing text messages or emails from SmarTone between August and December 2017 (in four months' time).

The complainant was a customer of SmarTone which provided mobile telecommunications service to her. In July 2017, she made her opt-out request to SmarTone relating to cessation of using her personal data in direct marketing by phone. However, the complainant still received a direct marketing email from SmarTone in August 2017 and hence complained to PCPD. During the period when PCPD was handling her complaint, the complainant continued receiving direct marketing text messages and emails from SmarTone. The Privacy Commissioner for Personal Data, Hong Kong was of the view that SmarTone failed to comply with the opt-out request of the complainant.

Related Regulation

Pursuant to section 35(3) of the Ordinance, a company which receives a customer's request for ceasing to use his or her personal data in direct marketing must comply with the request without charge. Failure to comply with the request is a criminal offence which is punishable by a fine of up to HK\$500,000 and imprisonment of up to 3 years.

無視客戶拒收促銷電話 和記電訊違私隱條例罰款2萬元

社會 22:30 2018/08/22 讚好 0

關注文章 儲存文章

分享: f d t w

熱門 愚人節 校長專欄 藍夢海奇 邵必豪啟事 李廷翰啟事 談太安啟事 新冠啟事 粵語精選 防範 粵語精選



▲無視客戶拒收促銷電話，和記電訊違私隱條例罰款2萬元。(資料圖片)

和記電訊旗下「3」的一名用戶於2016年5月已向提出拒收直銷訊息，惟同年6月及8月仍接獲「3」流動電話服務來電，遂公私隱專員公署作出投訴；和記電訊今日(22日)在於東區裁判法院被控違反兩項《私隱條例》，無依從資料當事人的拒收直銷訊息要求，並繼續使用其個人資料作直接促銷，和記電訊承認控罪，每項控罪分別被判罰款1萬元，即合共被判罰款2萬元。

私隱專員黃繼兒表示，為了有效地依從客戶的拒收直銷服務要求，服務供應商應備存一份拒收直銷訊息的客戶名單，並適時發放予相關同事，停止使用名單內的客戶資料作直銷用途，以及向員工提供適當的訓練等。

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



守護·私隱·廿五載
GUARDIAN · PRIVACY · 25 YEARS

Privacy Impact Assessment

- PIA is a systemic risk assessment tool
- Its objective is to avoid/ minimize adverse impacts on personal data privacy

When to conduct PIA?

Before introducing any new process involving personal data

Before any *material change* to the data user's existing personal data process

Where there is **material change** to regulatory requirements relating to personal data

Periodically

Material Change?

Collection of new types of personal data (due to new services or products)



Significant changes in the way personal data is used or disclosed (prescribed consent needed?)



Significant change to the access right of a system containing personal data



Outsourcing of data processing (include data storage)



Outsourcing of IT management, etc.

Identify & fix problems at an early stage

Help avoid reputational damage

Benefits of conducting PIA

Meet data subjects' expectations of privacy

Demonstrate compliance with your data protection obligations

PCPD



H K

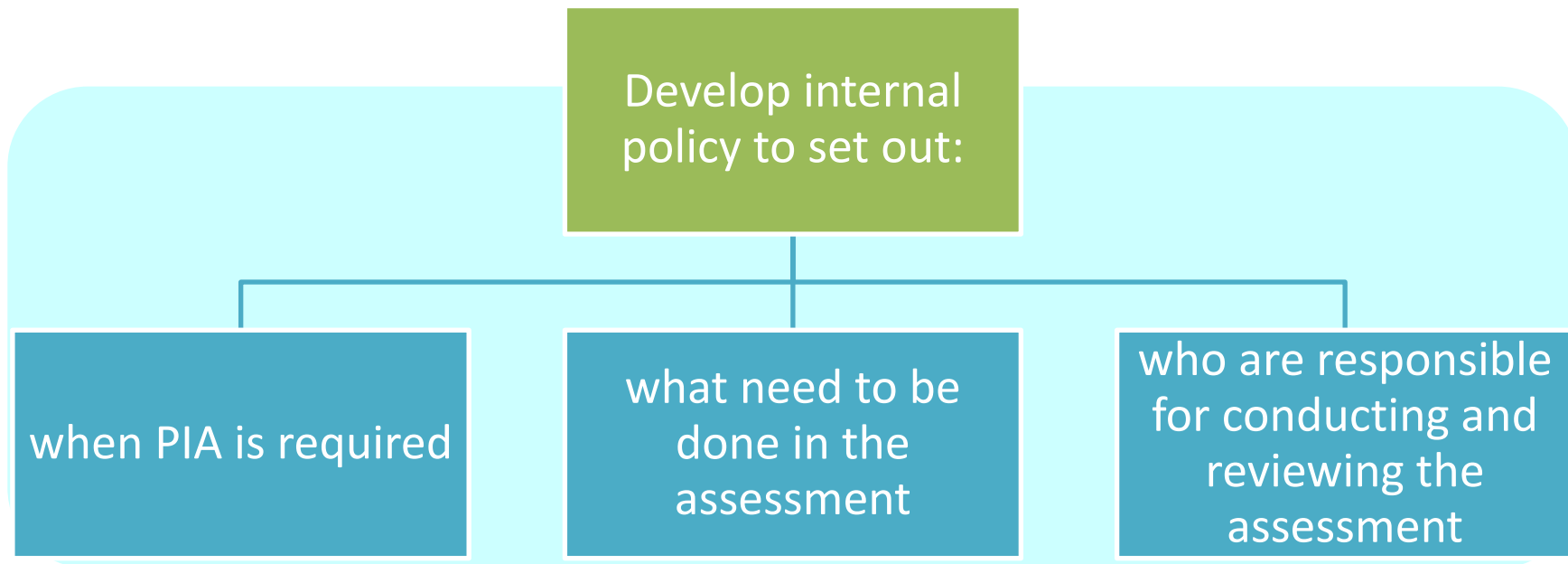


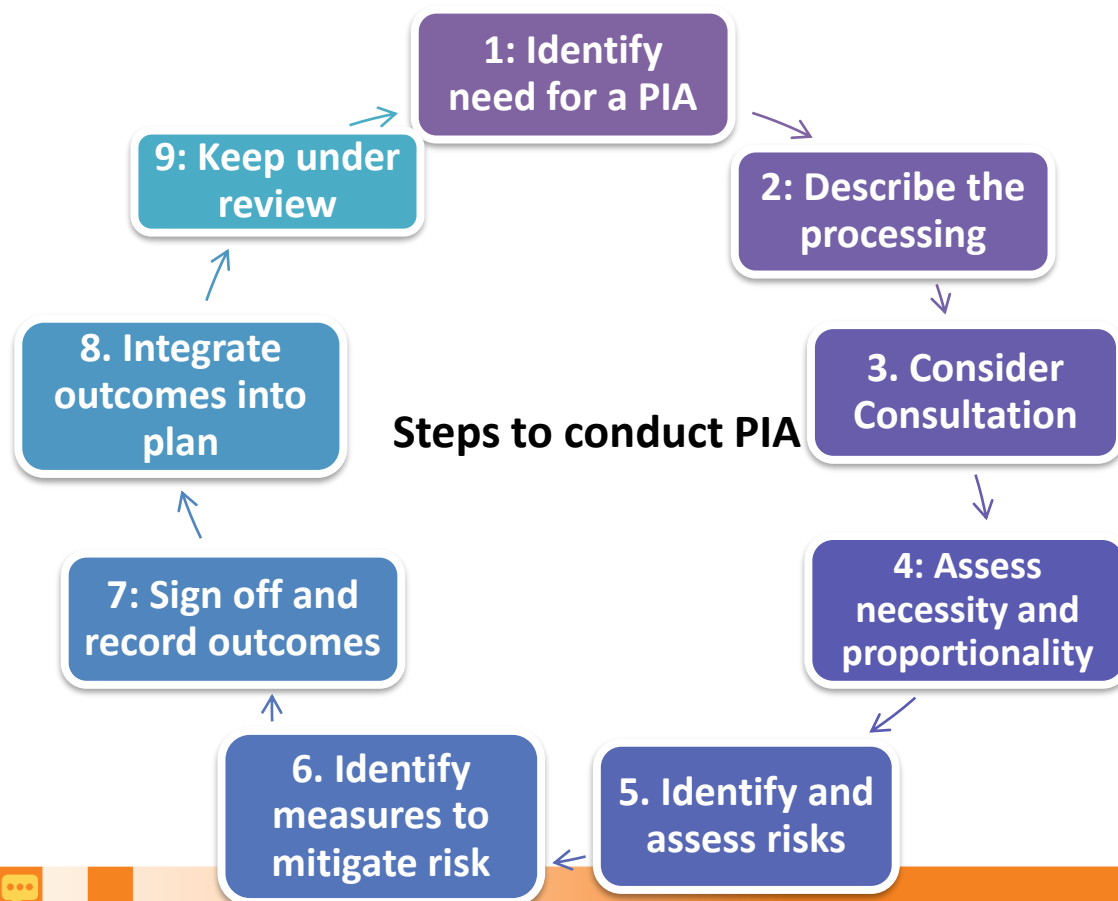
香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong



38

Policy on PIA





Checklists

PIA awareness check

Any training to ensure staff understand the need to consider a PIA?

Existing policies or procedures include references to PIA?

Staff understand when to conduct a PIA?

created and documented a PIA process?

Any training to staff on how to carry out a PIA?

Source: UK Information Commissioner's Office

41

Checklists

PIA process check

Did your PIA:

- describe the nature, scope, context , purposes and operation of the processing?
- mention who is the data user and data processor?
- cover **6** DPPs and describe how you will ensure compliance with DPPs
e.g. the collection of personal data is necessary for and proportionate to your purposes;
the exact retention period and justifications;
is the safeguard measures proportionate to the level of sensitivity of the personal data

42

Checklists

PIA process check

Did your PIA:

- do an objective assessment of the likelihood & severity of any risks to data subjects
- identify measures you can put in place to eliminate or reduce high risks
- record the decision-making in the outcome of the PIA, including any difference of opinion with your DPO or individuals consulted
- implement the measures you identified, and integrate them into your project plan
- keep your PIA under review and revisit them when necessary

43

Checklists

A good PIA should:

- ✓ specify why you need a PIA, detailing the types of intended processing that made it a requirement
- ✓ set out clearly the relationships between data users, processors, data subjects and systems, using both text and data-flow diagrams where appropriate
- ✓ ensure that the specifics of any flows of personal data between people, systems, organisations and countries have been clearly explained and presented

Checklists

A good PIA should:

- ✓ explicitly state how you are complying with each of the DPPs
- ✓ explain how you plan to support the relevant information rights of our data subjects
- ✓ identify all relevant risks to data subjects, assessed their likelihood and severity, and detailed all relevant mitigations
- ✓ evidence your consideration of any less risky alternatives to achieving the same purposes of the processing

Checklists

A good PIA should:

- ✓ attach any relevant additional documents you refer in the PIA, e.g. Privacy Notices, consent documents
- ✓ record the advice and recommendations of your DPO and ensure the PIA is signed off by the authorised person
- ✓ document a schedule for reviewing the PIA regularly

46

Information leaflet on PIA



Contact Us



Hotline

2827 2827

Fax

2877 7026

Website

www.pcpd.org.hk

E-mail

communications@pcpd.org.hk

Address

1303, 13/F, Dah Sing Financial Centre,
248 Queen's Road East,
Wanchai, HK

Copyright



This PowerPoint is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this PowerPoint, as long as you attribute the work to the Office of the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0.



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



Q&A session

PCPD



H K

PCPD.org.hk

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



守護 · 私隱 · 廿五載
GUARDIAN · PRIVACY · 25 YEARS

спасибо
danke 謝謝
ngiyabonga
teşekkür ederim
tapadh leat
dank je
gracias
mochchakkeram
go raibh maith agat
arigato
dakujem
merci
sukriya
kop khun krap
grazie
ευχαριστώ
terima kasih
감사합니다
obrigado
sagolun
dziękuję
hvala
mauruuru
bedankt

PCPD



H K

PCPD.org.hk

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



守護・私隱・廿五載
GUARDIAN · PRIVACY · 25 YEARS