

# Challenges for the Media – How to Safeguard Personal Data Privacy in the Digital Era?

Ms Stephanie Chau, Legal Counsel  
Office of the Privacy Commissioner for Personal Data  
18 March 2025

## Disclaimer

The information provided in this PowerPoint for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance (Cap 486) ("PDPO"). For a complete and definitive statement of law, direct reference should be made to the PDPO itself. The Office of the Privacy Commissioner for Personal Data makes no express or implied warranties of accuracy or fitness for a particular purpose or use with respect to the information set out in this PowerPoint. The contents provided will not affect the exercise of the functions and powers conferred to the Commissioner under the PDPO.

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



**1. Right to Privacy and Freedom of Press**

**2. Privacy in the Digital Age**

**3. Right to be Forgotten**

**4. Protect your Privacy on Social Media**

**5. Privacy and ethical risks arising from AI**



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





# Right to Privacy and Freedom of Press



# Right to Privacy

## Article 28 of the Basic Law

The freedom of the person of Hong Kong residents shall be inviolable.

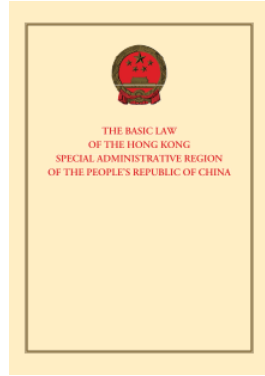
...

## Article 29 of the Basic Law

The homes and other premises of Hong Kong residents shall be inviolable. ...

## Article 30 of the Basic Law

The freedom and **privacy** of communication of Hong Kong residents shall be protected by law. 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.



## Article 12 of the Universal Declaration of Human Rights

No one shall be subjected to arbitrary interference with his **privacy**, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

## Article 14, Section 8, Part II of the Hong Kong Bill of Rights Ordinance (Cap. 383)

**Protection of privacy, family, home, correspondence, honour and reputation**

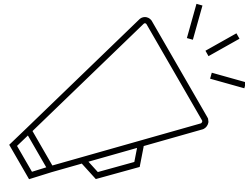
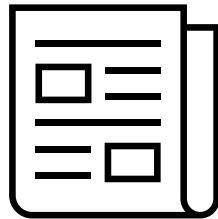
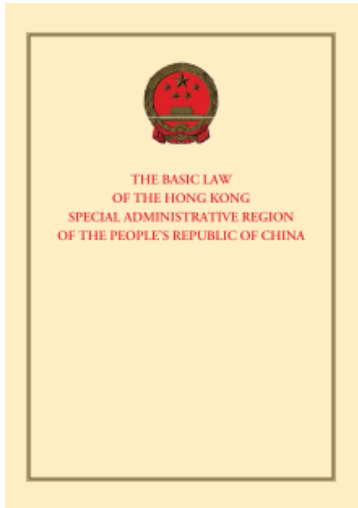
- (1) No one shall be objected to arbitrary or unlawful interference with his **privacy**, family, home or **correspondence**, nor to unlawful attacks on his honour and reputation.
- (2) Everyone has the right to the protection of the law against such interference or attacks.

[c.f. Article 17 of the International Covenant on Civil and Political Rights (“ICCPR”)]

# Freedom of Press

## Article 27 of the Basic Law

Hong Kong residents shall have **freedom of speech, of the press and of publication**; freedom of association, of assembly, of procession and of demonstration; and the right and freedom to form and join trade unions, and to strike.



## Article 16, Section 8, Part II of the Hong Kong Bill of Rights Ordinance (Cap. 383)

### Freedom of Opinion and Expression

- (1) Everyone shall have **the right to hold opinions without interference**.
- (2) Everyone shall have **the right to freedom of expression**; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.
- (3) The exercise of the rights provided for in paragraph (2) of this article **carries with it special duties and responsibilities**. It may therefore **be subject to certain restrictions**, but these shall only be such as are provided by law and are necessary
  - (a) for respect of the rights or reputations of others; or
  - (b) for the protection of national security or of public order (*ordre public*) or of public health or morals.

[c.f. Article 19 of the International Covenant on Civil and Political Rights ("ICCPR")]

# Right to Privacy and Freedom of Press

- Fundamental rights
- **Absolute rights?**

## Article 4 of the International Covenant on Civil and Political Rights (“ICCPR”)

No derogation from articles 6 [*right to life*], 7 [*freedom from torture and other cruel, inhuman or degrading treatment or punishment*], 8 (paragraphs I and 2) [*freedom from slavery and servitude*], 11 [*freedom from imprisonment for inability to fulfil a contractual obligation*], 15 [*prohibition against the retrospective operation of criminal laws*], 16 [*right to recognition before the law*] and 18 [*right to freedom of thought, conscience and religion*] may be made under this provision.

Must be **balanced** with other rights and the public interest

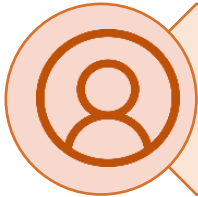


# Privacy in the Digital Age

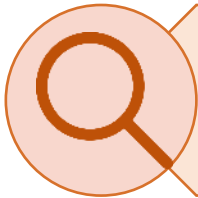


# “Personal Data”

## section 2 of the PDPO



Relating directly or indirectly to a **living individual**;



Practicable for the **identity** of the individual to be directly or indirectly **ascertained**; and



In a form in which **access to or processing of is practicable**



# Data Protection Principles (DPPs)

- All data users must comply with the six DPPs
- The six DPPs cover every item of personal data in the whole **data processing cycle**

收集目的及方式  
Collection  
Purpose & Means

1



準確性、儲存及保留  
Accuracy & Retention

2



使用  
Use

3



保安措施  
Security

4



透明度  
Openness

5



查閱及更正  
Data Access &  
Correction

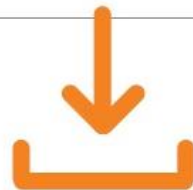
6



# 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。

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，而不超乎適度。

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

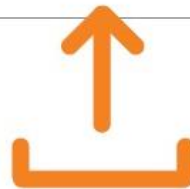
All practicable steps shall be taken to notify the data subjects of the purpose of data collection, and the classes of persons to whom the data may be transferred.

Data collected should be necessary but not excessive.

# Data Protection Principles (DPPs)

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.

*Re Hui Kee Chun CACV 4/2012*

*“52. ...(DPP3) is directed against the misuse of personal data and it matters not that the personal data involved has been published elsewhere or is publicly available. This is entirely consistent with the objective of the PDPO to protect personal data.”*

# Collection and Use of Personal Data Obtained from the Public Domain



## Guidance Note

### Guidance on Use of Personal Data Obtained from the Public Domain

#### Purpose of this guidance

This Guidance Note is intended to assist data users to comply with the requirements under the **Personal Data (Privacy) Ordinance** (the “**Ordinance**”) when collecting and using personal data from the public domain.

#### Personal data available in public domain

Personal data can be accessed and obtained from the public domain through different channels, e.g. a public register, a public search engine or a public directory, etc. A data user may do so for compiling information about an individual whom it targets or seeks to identify.

Below are some examples of use of personal data available in the public domain:

#### Examples:

1. A market research company uses personal data obtained from a public telephone directory to conduct surveys and publish reports.
2. A business entity provides its corporate customers with composite personal data of individuals aggregated from different public information sources.
3. An organisation develops a master index to facilitate the search by users of information it has compiled about an identified individual from websites, media releases, etc.

It is a misconception that publicly accessible personal data can be further used or disclosed for any purpose whatsoever without regulation.

The protection afforded by the Ordinance does apply to such personal data and there is no general exemption from compliance with the requirements under the Ordinance.

#### The legal requirements

A data user who collects and uses personal data from the public domain must observe the requirements under the Ordinance, in particular, **Data Protection Principle (“DPP”) 1(2)** and **DPP3**.

**DPP1(2)** requires personal data to be collected by means which are lawful and fair in the circumstances of the case. **DPP3** specifies that personal data shall not, without the prescribed consent of the data subject, be used for a new purpose. The term, “new purpose” in relation to the use of personal data, means in essence any purpose other than the one for which the personal data was originally collected or a directly related purpose. “Prescribed consent” means consent that is expressly and voluntarily given and has not been withdrawn by the data subject in writing. The term “use” in relation to personal data includes the disclosure and transfer of the data.

According to judicial authority, DPP3 “is directed against the misuse of personal data and it matters not that the personal data involved has been published elsewhere or is publicly available. This is entirely consistent with the objective of the [Ordinance] to protect personal data”<sup>1</sup>.

## • Collection

- Data users who make personal data available in the public domain may specify the circumstances or impose restrictions under which personal data may be accessed and used.
- A person who collects personal data from the public domain regardless of these stipulations and restrictions may contravene DPP1(2).

## • Use

- The fact that a data subject’s personal data can be obtained from the public domain shall not be taken to mean that the data subject has given blanket consent for use of his/her personal data for whatever purposes.

<sup>1</sup> See Judgment given by Hui Chu JA in *Re Hui Kee Chun*, CACV 4/2012, at para 52. The case concerns the publication on websites information regarding the full name, name of the employer and job position of a staff member in an educational institute along with a link to certain recorded conversations.

# Collection and Use of Personal Data Obtained from the Public Domain



*HKSAR v Choy Yuk Ling* FACCC 2/2023 (Date of judgment: 5 June 2023)

- The Appellant was charged with two counts of “knowingly making a false statement to obtain a certificate”, contrary to section 111(3)(a) of the Road Traffic Ordinance (Cap. 374)
- The falsity alleged was the appellant’s selection of the purpose of her application as “[o]ther traffic and transport related matters” in Step 2 of the application process (as described above), when in fact her real reason for applying for the certificate was for investigative journalism.

# Collection and Use of Personal Data Obtained from the Public Domain



*HKSAR v Choy Yuk Ling* FACCC 2/2023 (Date of judgment: 5 June 2023)

- Judgment:
  - In light of the principle against doubtful penalisation and the constitutionally protected freedom of speech and of the press, “Whilst such rights are not absolute and may be restricted where necessary, there is no reason to proceed from a starting point that **bona fide journalism** should be excluded from the phrase “other traffic and transport related matters”
  - The Appellant's statement as to the use of the application certificate was not a false statement.
  - It is not an irresistible inference that the Appellant knowingly made a false statement in stating the use of his application certificate because the phrase ‘other traffic and transport related matters’ is neither clear nor precise. Considering the number of certificates applied for and issued to media and news organisations, the Appellant, as a journalist, might well have honestly mistakenly believed that the use of his journalistic work was covered by the term ‘other traffic and transport related matters’.

# Exemption of “news activity”

- To strike a balance between upholding freedom of the press and protection of personal data privacy rights

## Section 61(2) of the PDPO

Personal data is exempt from **DPP3** in any case in which—

- (a) the **use of the data** consists of disclosing the data to a data user whose business (or part of whose business) consists of a **news activity**; and
- (b) such disclosure is made by a person who has **reasonable grounds to believe** (and reasonably believes) that the publishing or broadcasting (wherever and by whatever means) of the data (and whether or not it is published or broadcast) is in the **public interest**.

## Section 61(3) of the PDPO

**News activity** (新聞活動) means any journalistic activity and includes –

- (a) the (i) gathering of news; (ii) preparation or compiling of articles or programmes concerning news; or (iii) observations on news or current affairs, for the purpose of dissemination to the public; or
- (b) The dissemination to the public of (i) any article or programme or concerning news; or (ii) observations on news or current affairs.

# Exemption of “news activity”

*Face Magazine Limited v PCPD & Sudden Weekly Limited v PCPD*  
(AAB Nos. 5&6/2012)(Date of decision: 6 January 2014)

- 3 celebrities complained that photos of their daily lives and intimate acts at home were taken at a place outside their home, and were published in a magazine without their consent
- Administrative Appeals Board:
  - the "*mere fact that a person is an artiste or is engaged in some occupation which brings him into public notice is not of itself enough to make his private life a matter of public interest*"; “*what may interest the public is not necessarily something in the public interest*”
  - **not in the public interest** to take and publish photographs showing the celebrities daily life and intimate acts at their private premises
  - Contravention of DPP1(2) – unfair collection of personal data
  - S.61 of the PDPO does not offer any exemption to news organisations from DPP1(2).



# Joint Code of Ethics of the 4 Journalistic Organisations

“(4) Journalists should **respect the reputation and privacy of individuals**. Taking into account public interest, journalists should report on the private life of individuals – who have not given their consent for doing so – only in ways that would **not exacerbate unnecessary additional damages to the individuals**.

4.1. **Privacy of children** should be **handled especially with great care**. Media organisations should have full grounds when reporting the contents about private lives of children. Journalist should not disclose the privacy of children purely because of the social or political status of the minors’ family or guardians.

4.2. Journalists should have **full grounds** reporting the behaviour and personal data of public figures.”

# Offences for disclosing personal data without consent

## s.64 of the PDPO

### Section 64(1) of the PDPO

A person commits an offence if the person discloses any personal data of a **data subject** which was obtained from a **data user** without the **data user's consent**, with an intent –

- (a) to obtain gain in money or other property, whether for the benefit of the person or another person; or
- (b) to cause loss in money or other property to the data subject.

### Section 64(3) of the PDPO

A person who commits an offence under subsection (1) is liable on conviction to a fine of \$1,000,000 and to imprisonment for 5 years.



# Offences for disclosing personal data without consent s.64 of the PDPO

*HKSAR v Next Digital Limited & Others* KTS 566-569/2021  
(Conviction and sentence: 15 June 2021)

- A reporter gained access to a birth certificate certified copy pertaining to the victim's son from the **Immigration Department** and published the details of the birth entry concerned in a magazine without the consent from the **data user**.
- Case result:
  - D1 – D3 (the two magazine companies and the chief editor) – **convicted** under s.64(1) of the PDPO upon guilty plea, fined HK\$40,000 each.
  - D4 (the reporter) – **12-month bind over** for HK\$2,000.



The screenshot shows a news article from the website 'eJINSIGHT'. The article title is '涉查冊刊張柏芝子出世紙 《壹週刊》2人被控'. The article text states that '壹週刊' (Yes Weekly) was charged for publishing a birth certificate of Angelina Cheung's son without her consent, violating the Privacy Ordinance. The article also mentions that the magazine's editor and a data collector were charged. The article is dated February 20, 2021, and is categorized as a '時事脈搏' (Social Pulse) article.

# Offences for disclosing personal data without consent

## s.64 of the PDPO



Effective from 8 Oct 2021

	First-tier – Summary Offence (section 64(3A) of the PDPO)	Second-tier – Indictable Offence (section 64(3C) of the PDPO)
1.	Any personal data of a data subject is disclosed <b>without the relevant consent</b> of the <b>data subject</b>	
2.	Has an <b>intent</b> or is being <b>reckless</b> as to whether <b>any specified harm</b> would be, or would likely be, caused to the data subject or any family member of the data subject	
3.	N/A	The <b>disclosure causes any specified harm</b> to the data subject or any family member of the data subject
<b>Penalty</b>	a fine at level 6 (HK\$100,000) and imprisonment for <b>2 years</b>	a fine of HK\$1,000,000 and imprisonment for <b>5 years</b>

# Offences for disclosing personal data without consent s.64 of the PDPO

- “Specified harm” – Sections 64(6) of the PDPO:

*Effective from 8 Oct 2021*



- Harassment, molestation, pestering, threat or intimidation to the person;



- Bodily harm or psychological harm to the person;



- Harm causing the person reasonably to be concerned for the person's safety or well-being; or



- Damage to the property of the person

# Offences for disclosing personal data without consent

## s.64 of the PDPO

*Effective from 8 Oct 2021*

- **Defence – Sections 64(4) of the PDPO:**

(a) the person reasonably believed that the disclosure was necessary for the purpose of **preventing or detecting crime**;

(b) the disclosure was required or authorized by or under any enactment, by any rule of law or by an order of a court;

(c) the person reasonably believed that the disclosure was made with the **relevant consent** of the data user (s.64(1))/ data subject (s.64(3A)/ (3C));

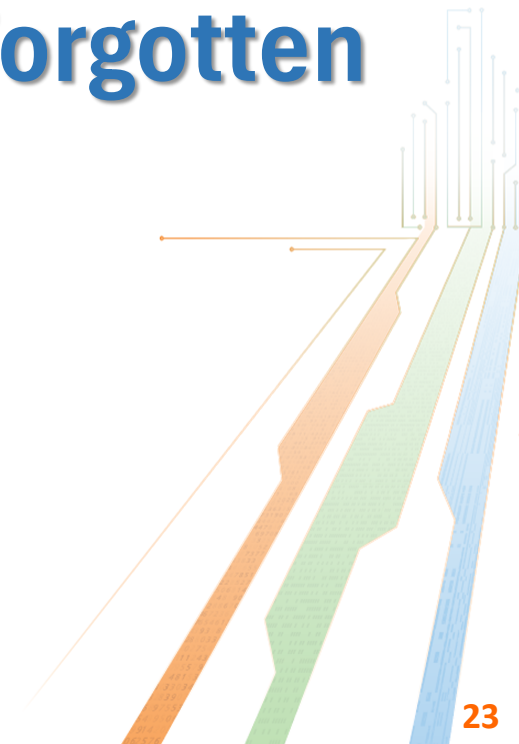
(d) the person disclosed the personal data solely for the purpose of a **lawful news activity** and has reasonable grounds to believe that such disclosure was in the public interest.

As defined under s.61(3) of the PDPO

# Would news activity constitutes “doxxing”?

- **Criminal act:**
  - **Disclosure** of personal data of a data subject without the relevant consent of the data subject?
- **Criminal intent:**
  - With an **intent** to cause any **specified harm** to the data subject or any family member of the data subject; or
  - Being **reckless** as to whether any **specified harm** would be, or would likely be, caused to the data subject or any family member of the data subject?
- **Defence:**
  - Disclosure of the personal data solely for the purpose of a **lawful news activity** and has reasonable grounds to believe that such disclosure was in the **public interest**?

# Right to be Forgotten





# Right to be Forgotten

## Article 17 of the General Data Protection Regulation (“GDPR”)

### Right to Erasure (“right to be forgotten”)

1. The data subject shall have the right to obtain from the **controller** the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies...
  - (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  - (b) the data subject withdraws consent on which the processing is based, and where there is no other legal ground for the processing;
  - (c) the data subject objects to the processing, and there is no overriding legitimate grounds for the processing;
  - (d) the personal data have been unlawfully processed;
  - (e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
  - (f) ...

# Right to be Forgotten

Hong Kong? – no independent “right to be forgotten” under the PDPO:  
X v PCPD (AAB Nos. 15/2019)(Date of decision: 7 August 2020)

## DPP2, Schedule 1 of the PDPO

### **Accuracy and duration of retention of personal data**

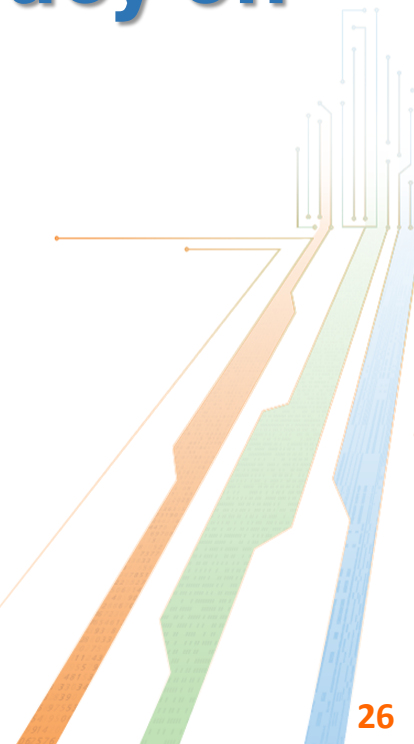
- requires data users to take all practicable steps to ensure that personal data is accurate and is not kept longer than is necessary for the fulfillment of the purpose for which the data is used

## Section 26 (1) of the PDPO

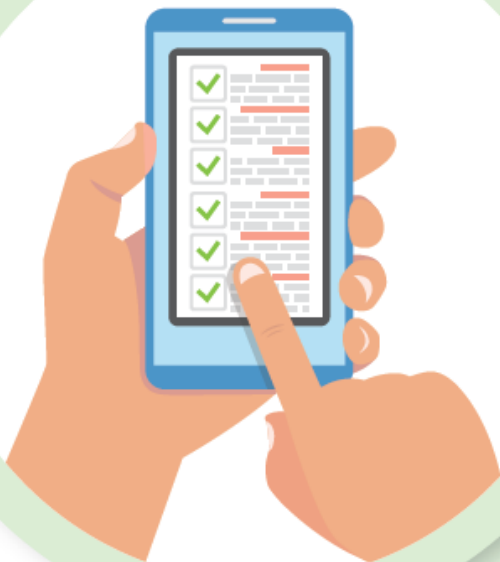
### **Erasure of personal data no longer required**

- requires data users to take all practicable steps to erase personal data that is no longer required for the purpose for which the data is used, unless erasure is prohibited by law or is not in the public interest
- could be engaged when a data user fails to respond to a complaint or request from a data subject for erasure of personal data

# Protect Your Privacy on Social Media



# Protect Your Privacy on Social Media



## Before registering for an account:

- ✓ Read the privacy policy
- ✓ Use a dedicated email account for registration
- ✓ Minimise the provision of personal data
- ✓ Set strong passwords
- ✗ Use the same password for different social media accounts
- ✗ Use other social media accounts for registration
- ✗ Share accounts and passwords with others

# Protect Your Privacy on Social Media

## After registering for an account:

- ✓ Check the default security or privacy settings and readjust the settings when necessary
- ✓ Activate two-step authentication function
- ✓ Adjust the app permission settings according to practical needs
- ✗ Reveal excessive personal information on social media, e.g. residential address, date of birth, telephone numbers and daily whereabouts



# Protect Your Privacy on Social Media



## When using the account:

- ✓ Log in regularly to check the privacy settings, back-up personal data and erase search history
- ✓ Look out for data breaches and failed log-in attempts
- ✓ Update the applications to the latest version
- ✗ Accept suspicious follower/ message requests
- ✗ Connect to public Wi-Fi
- ✗ Download applications from unofficial sources
- ✗ Keep unused accounts

# Protect Your Privacy on Social Media

## 社交媒體：私隱保障實用貼士 Practical Tips on Privacy Protection In Using Social Media

- 細閱私隱政策  
Read the privacy policy
- 切勿發布或轉載「起底」訊息  
Do not publish or forward doxing messages
- 檢查預設私隱及保安設定  
Check the default settings on privacy and security
- 採用強密碼及啟用雙重認證功能  
Use strong passwords and enable two-factor authentication
- 如非必要，關閉位置追蹤功能  
Turn off the location tracking function if not needed
- 避免使用公共Wi-Fi進行交易  
Avoid transactions over public Wi-Fi connections

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

APPA PRIVACY 11-17 2022

## Protect Your Personal Data Be Smart on Social Media

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

## 社交媒體私隱設定 大檢閱

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

## Sharenting Dos and Don'ts

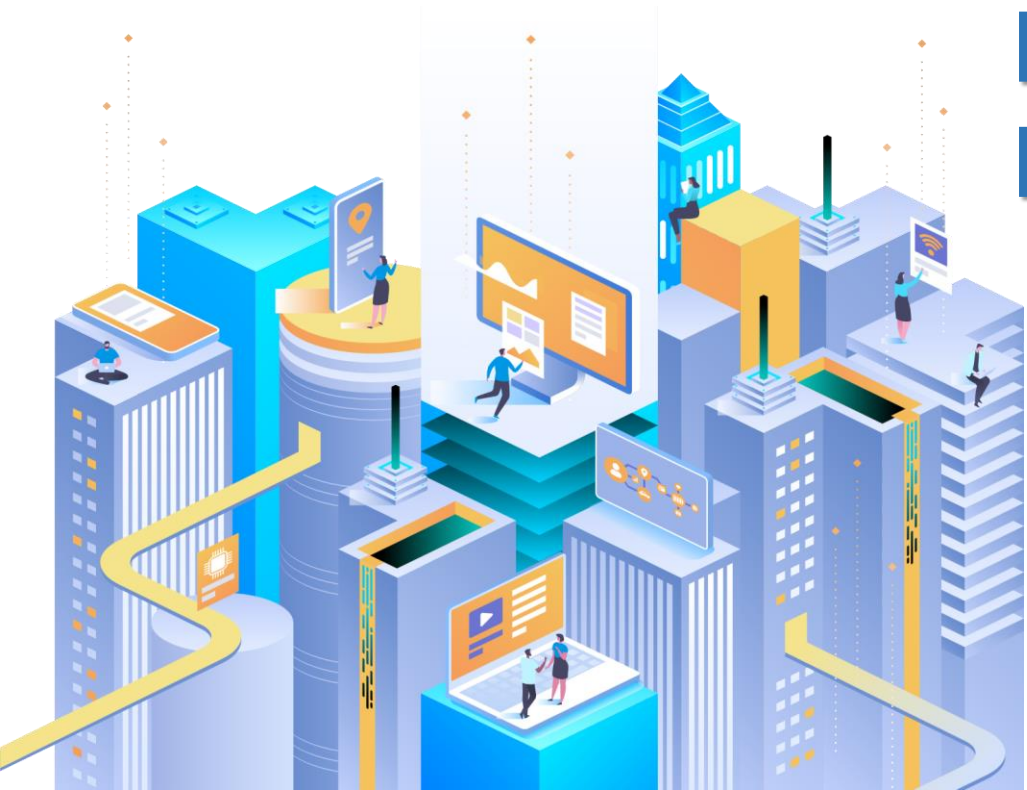
What is "sharenting"? If you always share your children's daily lives on social media platforms, you may be engaged in sharenting ("sharing" + "parenting"). This pamphlet provides you with some dos and don'ts in sharenting.

**Dos**

- Beware of the details:** Take a second look at your social media post before publishing to make sure it does not reveal any personal details of your children or that of others, e.g., full facial image, full name, date of birth, student number, name of school / teacher, etc.
- Communicate - Seek agreement:** Consider asking for your children's consent before posting to show your respect for their willingness. If your children feel upset or embarrassed about the posts you shared, remove the posts immediately.
- Double check your privacy settings:** Make sure that appropriate privacy settings are in place, such as whether your posts are visible to the public or just a confined group. Check whether a social media platform's privacy policy allows correction and/or erasure requests to be made.
- Think about the future:** Think twice before sharing your children's information. Consider whether you want the post to be part of your children's digital footprint. Would it cause embarrassment to the children in the future or affect their education or work prospects?

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

# Privacy and Ethical Risks arising from AI





# Privacy Risks arising from AI

**1 Excessive data collection**

- Data collected for AI may include PD



**3 Use of data**

- Users hard to understand how PD is used



**2 Identity re-identification**

- Possible to re-identify individuals by collecting and matching data from different sources



**4 Data repurposing**

- Data gathered for a specific purpose is used for another one



**5 Data breach**

- Vast amounts of PD in AI systems
- Big impact if breached



**6 Excessive retention period**

- Data retained for longer than necessary for the original purpose



# Ethical Risks arising from AI

1

## Bias & discrimination



- Poor data quality and accuracy in training data
- Biased data leading to discriminatory outcomes

2

## Hallucination



- Large language models creating outputs that are nonsensical or inaccurate

3

## Explainability

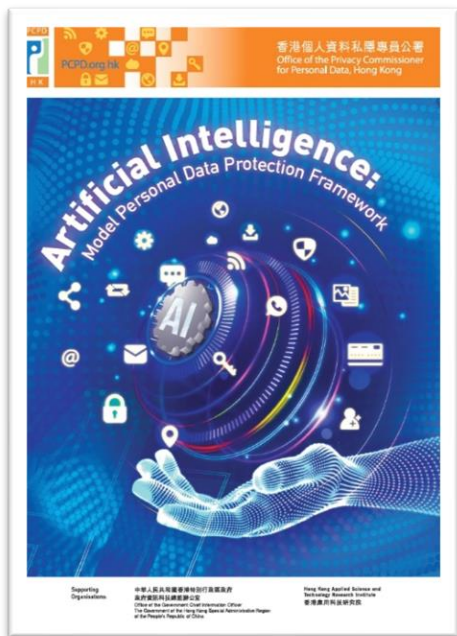


- “Black-box”
- Lack of transparency

# Artificial Intelligence: Model Personal Data Protection Framework

## Business-friendly

## Benefits



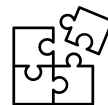
**Best practices**



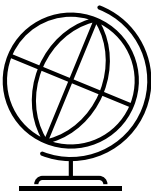
**Assist organisations in complying with the requirements of the Personal Data (Privacy) Ordinance**



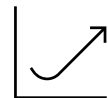
**Risk-based approach**



**Facilitate Hong Kong's development into an innovation & technology hub**



**Alignment with international standards**



**Nurture the healthy development of AI in Hong Kong**



**Propel the expansion of the digital economy not only in HK but also GBA**

# 咁大隻蛤乸

# 隨街跳?

Too good to be true?

## 個人資料亂俾 踢走騙徒靠晒你

Don't Hand Over Your Personal Data  
Beware of Fraudsters

個人資料防騙熱線 3423 6611  
Personal Data Fraud Prevention Hotline



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



防騙特工  
馮素波



即睇防騙短片  
Scan to watch the  
anti-fraud videos

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



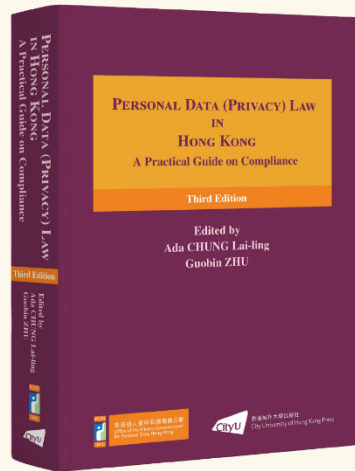
**Ms Ada CHUNG Lai-ling**  
Privacy Commissioner for Personal Data,  
Hong Kong



**Professor ZHU Guobin**  
Professor ZHU Guobin  
City University of Hong Kong

# PERSONAL DATA (PRIVACY) LAW IN HONG KONG

## A Practical Guide on Compliance (Third Edition)



### Highlights:

- Provisions of the PDPO on combatting doxxing
- Cross-border transfers of personal data from Hong Kong
- The Mainland's personal information protection regime
- Recent decisions by the Administrative Appeals Board and the Court
- PCPD's investigation reports and materials
- Comparison table on the personal data protection laws of Hong Kong, the Mainland and the European Union

Buy Now



# 《私隱法·保 — 了解你的個人資料私隱》

## “The Treasure-trove of Privacy – Understanding Your Personal Data Privacy”

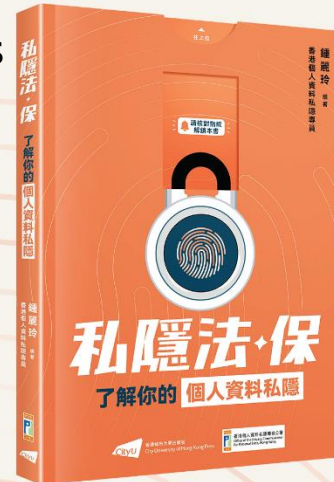


**Ms Ada CHUNG Lai-ling**

Privacy Commissioner for Personal Data,  
Hong Kong

### Highlights:

- Data Protection Principles
- Combating Doxxing
- Trends of Privacy Protection
  - ◆ Artificial Intelligence
  - ◆ Chatbot
- Savvy Tips for Protecting Privacy



Buy Now



# Contact Us

 **Hotline** 2827 2827

 **Fax** 2877 7026

 **Website** [www.pcpd.org.hk](http://www.pcpd.org.hk)

 **Email** [communications@pcpd.org.hk](mailto:communications@pcpd.org.hk)

 **Address** Unit 1303, 13/F, Dah Sing Financial Centre, 248 Queen's Road East, Wanchai, Hong Kong

保障、尊重個人資料私隱

*Protect, Respect Personal Data Privacy*

追蹤我們  
最新資訊

