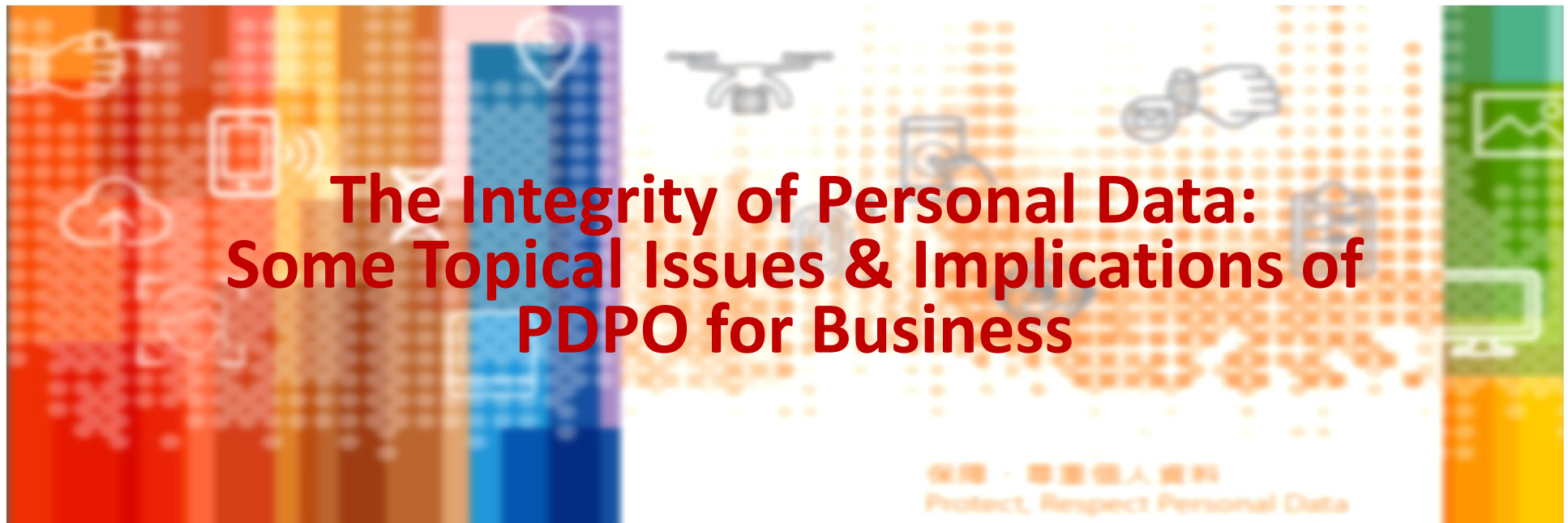


**Democratic Alliance for  
the Betterment and Progress of Hong Kong**  
**21.04.2018**



**Stephen Kai-yi Wong, Barrister**  
**Privacy Commissioner for Personal Data, Hong Kong**

A stylized illustration of a man with a large, grey, bushy mustache and a white beard. He has a neutral expression with two small black dots for eyes and a simple white line for a mouth. He is wearing a red and white checkered shirt. In his right hand, he holds a brown telephone receiver with a coiled cord. Above his head is a thought bubble containing a white padlock icon, suggesting a connection between the man and the concept of security. The background is a solid light blue color.

# Data Security

# 黑客入侵 香港寬頻 失38萬客戶資料

有黑客盜取商業機密客戶資料，曾經糾纏香港寬頻的，更要求快報責有否受影響！香港寬頻公布，周一發現黑客入侵一個存有已停用客戶資料的伺服器，涉及38萬名客戶個人資料，佔公司360萬客戶紀錄逾11%，當中更有4.3萬人的信用卡資料相傳已外泄。案件由警方網絡安全及科技罪案調查科跟進，初步調查顯示，暫不涉勒索。外界關注停用的客戶資料為何未有刪除及極易被入侵，疑資料未有加密，香港寬頻僅以正進行調查為由，未有交代。

## 個人資料被盜事件簿

Source: <http://www.pcpd.org.hk>

- 今年1月一銀行發生電腦系統被黑客入侵事件，涉及高約10萬名客戶資料，損失逾100萬元。
- 去年11月一銀行發生電腦系統被黑客入侵事件，涉及高約10萬名客戶資料，損失逾100萬元。
- 去年11月一銀行發生電腦系統被黑客入侵事件，涉及高約10萬名客戶資料，損失逾100萬元。
- 去年11月一銀行發生電腦系統被黑客入侵事件，涉及高約10萬名客戶資料，損失逾100萬元。
- 去年11月一銀行發生電腦系統被黑客入侵事件，涉及高約10萬名客戶資料，損失逾100萬元。



PCPD

PCPD.org.hk est.1996

HK



警方調查發現，盜取資料的黑客，曾利用多個IP地址，向香港寬頻的伺服器發動攻擊。警方表示，目前尚不清楚黑客的動機，但資料顯示，黑客在入侵後，曾嘗試刪除資料，但被系統自動備份功能阻止。警方呼籲客戶，如有任何資料外泄，請立即向警方舉報。

## 香港寬頻泄客戶資料 私隱專員：以全球營業額作罰則是大勢所趨

Source: <https://goo.gl/bwGb3r>

香港寬頻疑被黑客入侵客戶資料庫，導致客戶個人資料外泄，涉及約38萬條固網及IDD客戶及服務申請者紀錄，當中包括2018年4月18日 星期三 萬條信用卡資料。個人資料在香港寬頻通報前，已主動有違返《個人資料(私隱)條例》。

黃繼兒在商台節目提醒，受影響客戶應立即聯絡銀行更改密碼，以

## 【今次大鑊了】香港寬頻：疑被黑客入侵 近38萬名客戶資料被盜 (16:43)

Source: <https://goo.gl/PiQiyt>

黃繼兒承認，香港有關私隱歐美一些國家已不斷修訂條，港未有類似懲罰機制。他認為，以全球營業額作罰阻嚇作用不大。他又表示，今次個香港寬頻通報時間算



## Principle 4 – Security of personal data

- Data users shall take **all practicable steps** to **safeguard** personal data against unauthorised or accidental access, processing, erasure, loss or use

## Principle 2 – Accuracy and duration of retention of personal data

- **DPP2(2):** Data users shall take **all practicable steps** to ensure personal data is **not kept longer than is necessary** for the fulfillment of the purpose for which the data is or is to be used



# Social Media Privacy

# Misuse of Personal Data by Social Media

## Facebook被揭截取Android用戶通話記錄

2018-03-27

#Hashtags Facebook Android



2018年03月18日 17:58 星期日

國際

【國際新聞】Facebook被揭疏忽處理用戶資料 英美立案調查

### Facebook被揭疏忽處理用戶資料 英美立案調查

讚好 0 分享

社交媒體Facebook因捲入英國政治諮詢公司Cambridge Analytica聞風波，再勾起用戶關注個人私隱。早前有用戶向Facebook取得社料，竟發現該公司收集了兩年的Android手機通話記錄。

Facebook被揭發有大量用戶資料落入大數據公司「劍橋分析」(Cambridge Analytica) 手上，涉嫌影響美國大選結果。美國政界要求盡快立法監管社交媒體，美國麻省司法部和英國信息專員辦公室均表示會對此立案調查。

民主黨參議員克羅布查 (Amy Klobuchar) 批評，fb沒有能力自我監察，fb行政總裁朱克伯格 (Mark Zuckerberg) 應到國會應訊。參議員華納 (Mark Warner) 則認為，如不立法監管社交媒體，該市場會缺乏透明度，很容易被用作不法用途。

Source: <https://goo.gl/kFXwcf>

The Switch

## U.S. and British lawmakers demand answers from Facebook chief executive Mark Zuckerberg

By Craig Timberg and Tony Romm March 18 Email the author

回上頁 | 友善列印

T T T

上一篇 | 下一篇



Mark Zuckerberg has kept a low profile as controversy over the political uses of the social media platform has

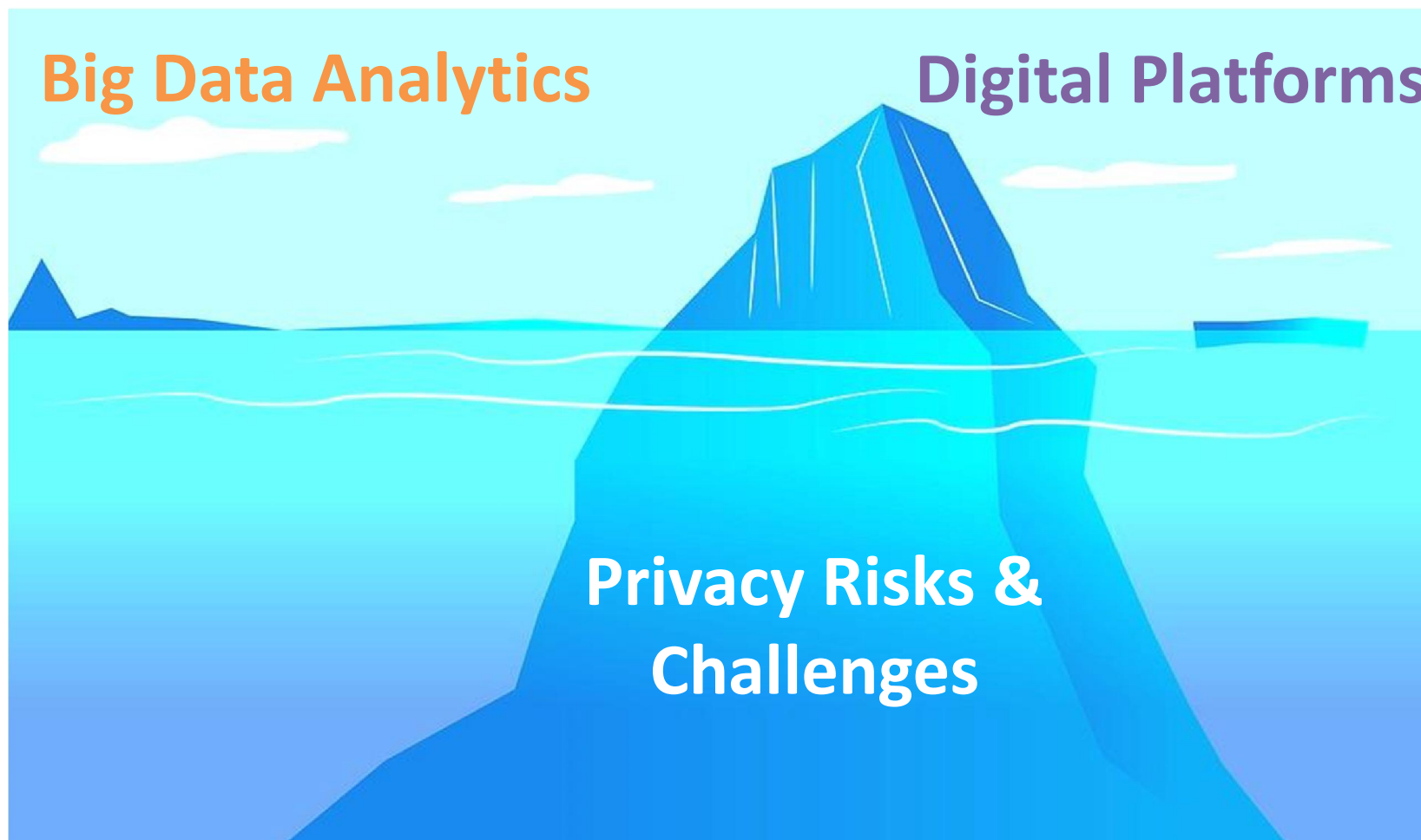
States and Britain are calling on Facebook chief executive Mark Zuckerberg to disclose preferences and other information from tens of millions of users ended up in the hands of the campaign connected with President Trump's 2016 campaign.

Source: <https://goo.gl/ZR3AqJ>

Source: <https://goo.gl/eNlt53>

7

# Privacy Risks and Challenges



8



# Ubiquitous and Covert Data Collection



**Data Minimization**

**Data Transparency**



**Adequate Notification**



**Erodes Individuals' Control Over Data**

9

# Unpredictable Analytics



**✗ Notice & Consent**



**✗ Purpose & Use Limitations**

10

# Profiling



## Re-identification



## ✘ Distinction between Personal Data & Non-Personal Data

11

# Inaccurate Inferences and Predictions

**✗ Data Accuracy**

**Filter Bubble**

**Interference in Elections...**

12



A stylized illustration of a man's face and upper torso. He has a large, light-colored head with a dark beard and mustache. He is wearing a red and white checkered shirt. He is holding a yellow telephone receiver to his ear. The background is a light blue color with some orange circles and a white cross symbol in the top right corner.

# **Global Data Protection Landscape - European Union General Data Protection Regulation (GDPR)**



# PDPO – GDPR Comparative Study

## Background


- **Keep abreast of overseas** privacy law developments
- **Assess GDPR's impact on businesses** (in particular multi-national organisations)
- **Comparable legal framework for** and commercial activities

14




# PDPO – GDPR Comparative Study

## Major differences between PDPO and GDPR:

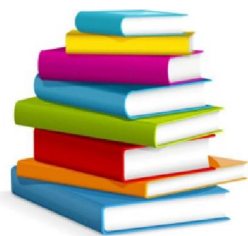
	EU	HK
<b>Application</b> 	<b>Data processors or controllers:</b> <ul style="list-style-type: none"><li>• with an establishment in the EU, or</li><li>• established outside the EU, that offer goods or services to, or monitor the behaviour of individuals in the EU. [Art 3]</li></ul>	<b>Data users (controllers /processors) who, either alone or jointly or in common with other persons, control the collection, holding, processing or use of the personal data in or from Hong Kong. [s.2(1)]</b>




# PDPO – GDPR Comparative Study

	EU	HK
<p><b>Personal Data</b></p> 	<p>"Personal data" means</p> <ul style="list-style-type: none"> <li>• any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly.</li> <li>• examples of personal data explicitly identified being extended to include location data and online identifier.</li> </ul> <p>[Art 4(1)]</p>	<p>"Personal data" means any data –</p> <ul style="list-style-type: none"> <li>• relating directly or indirectly to a living individual;</li> <li>• from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and</li> <li>• in a form in which access to or processing of the data is practicable.</li> </ul> <p>[s.2(1)]</p>






## PDPO – GDPR Comparative Study

	EU	HK
<p><b>Accountability and Governance</b></p> 	<p>Risk-based approach; data controllers are required to:</p> <ul style="list-style-type: none"> <li>• implement technical and organisational measures to ensure compliance [Art 24];</li> <li>• adopt data protection by design and by default [Art 25];</li> <li>• conduct data protection impact assessment for high-risk processing [Art 35]; and</li> <li>• (for certain types of organisations) designate Data Protection Officers. [Art 37]</li> </ul>	<p>The accountability principle and the related privacy management measures are not explicitly stated. The Privacy Commissioner advocates the adoption of a privacy management programme which manifests the accountability principle. The appointment of data protection officers and the conduct of privacy impact assessment are recommended good practices for achieving accountability.</p>




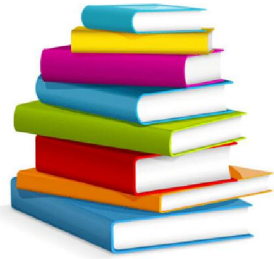
## PDPO – GDPR Comparative Study

	EU	HK
<b>Sensitive Personal Data</b> 	Category of sensitive personal data expanded. Processing of sensitive personal data is allowed only under specific circumstances. [Art 9]	No distinction between sensitive and non-sensitive personal data for all purposes.




# PDPO – GDPR Comparative Study

	EU	HK
<p><b>Consent</b></p> 	<p>Consent must be</p> <ul style="list-style-type: none"> <li>• freely given, specific and informed;</li> <li>• an unambiguous indication of a data subject's wishes, by statement or by clear affirmative action, which signifies agreement [Art 4(1)]; and</li> <li>• given by a child below 16 (or 13) with parental authorisation.</li> </ul>	<p>Consent is not a pre-requisite for the collection of personal data, unless the personal data is used for a new purpose.[DPP1&amp;3] For other purposes, where consent is also required, consent means express and voluntary consent.</p> <p>No requirement for parental consent.</p>




## PDPO – GDPR Comparative Study

	EU	HK
<p><b>Breach Notification</b></p> 	<p>Data controllers are required to notify the authority of a data breach without undue delay (exceptions apply).</p> <p>Data controllers are required to notify affected data subjects if it is likely to result in high risk to the rights and interests of the data subjects, unless exempted. [Arts 33-34]</p>	<p>No mandatory requirement, but notification to the Privacy Commissioner (and data subjects, where appropriate) is recommended in the interest of all stakeholders including data users/controllers and subjects.</p>






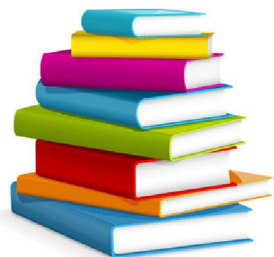
## PDPO – GDPR Comparative Study

	EU	HK
<p><b>Data Processors</b></p> 	<p>Data processors are additionally obliged to maintain records of processing, ensure security of processing, report data breaches, designate Data Protection Officers, etc. [Arts 30, 32-33, 37]</p>	<p>Data processors are not directly regulated. [s.2(12)] Data users are required to adopt contractual or other means to ensure data processors' compliance. [DPP2(3) &amp; DPP4(2)]</p>




## PDPO – GDPR Comparative Study

	EU	HK
<p><b>New and Enhanced Rights for Data Subjects</b></p> 	<ul style="list-style-type: none"> <li>• Right to notice on data processing. [Art 13-14]</li> <li>• Right to erasure of personal data ("right to be forgotten"). [Art 17]</li> </ul>	<ul style="list-style-type: none"> <li>• Less extensive notice requirements for data users / controllers (processors).</li> <li>• No right to erasure, but data shall not be retained longer than necessary. [s.26 &amp; DPP 2(2)]</li> </ul>




## PDPO – GDPR Comparative Study

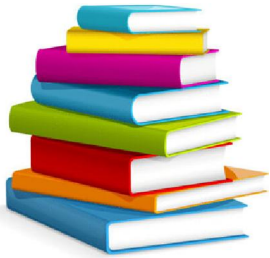
	EU	HK
<p><b>New and Enhanced Rights for Data Subjects (con't)</b></p> 	<ul style="list-style-type: none"><li>• Right to restriction of processing and data portability. [Art 18, 20]</li><li>• Right to object to processing (including profiling). [Art 21]</li></ul>	<ul style="list-style-type: none"><li>• No right to restriction of processing and data portability, but data access and correction requests be complied with. [DPP6, Part 5]</li><li>• No right to object to processing (including profiling), but may opt out from direct marketing activities [ss.35G &amp;35L] and PDPO contains provisions regulating data matching procedure. [ss.30-31]</li></ul>




## PDPO – GDPR Comparative Study

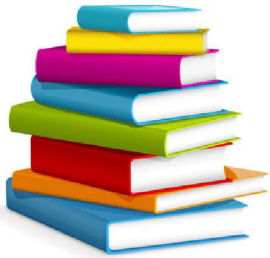
	EU	HK
<b>Certification, Seals, and Codes of Conduct</b> 	Mechanisms are explicitly recognised and established for demonstrating compliance by data controllers and processors. [Art 42]	No formal recognition of certification or privacy seals mechanisms for demonstrating compliance. The Privacy Commissioner may approve and issue code of practice after consultation. [s.12]






## PDPO – GDPR Comparative Study

	EU	HK
<b>Cross-jurisdiction Data Transfer</b> 	Certification and adherence to approved codes of conduct are explicitly made one of the legal bases for transfer. [Art 46]	Certification and adherence to an approved code of practice are not explicitly made a legal basis.



## PDPO – GDPR Comparative Study

	EU	HK
<p><b>Sanctions</b></p> 	<p>Data protection authorities are empowered to impose administrative fines on data controllers and processors. [Art 58]</p> <p>Depending on the nature of the breach, the fine could be up to €20 million or 4% of the total worldwide annual turnover. [Art 83]</p>	<p>The Privacy Commissioner is not empowered to impose administrative fines or penalties. The Privacy Commissioner may serve Enforcement Notices on data users, failure to comply with which may attract penalties after judicial process. [s.50]</p>

# “European Union General Data Protection Regulation 2016” Booklet



[www.pcpd.org.hk//tc\\_chi/resources\\_centre/publications/files/eugdpr\\_c.pdf](http://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/eugdpr_c.pdf)



[www.pcpd.org.hk//english/resources\\_centre/publications/files/eugdpr\\_e.pdf](http://www.pcpd.org.hk//english/resources_centre/publications/files/eugdpr_e.pdf)



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

A stylized illustration of a man's face and upper torso. The man has a large, round, light-colored head with a dark mustache and a small white mustache above it. He is wearing a red and white checkered shirt. He is holding a yellow telephone receiver in his right hand. The background is a light blue gradient. There are some orange circles and a white cross-like shape in the upper right corner.

# Person-to-person Telemarketing Calls



# Regulated by PD(P)O?



made to phone numbers  
randomly generated



made to specific individuals  
by using their names and phone  
numbers

29

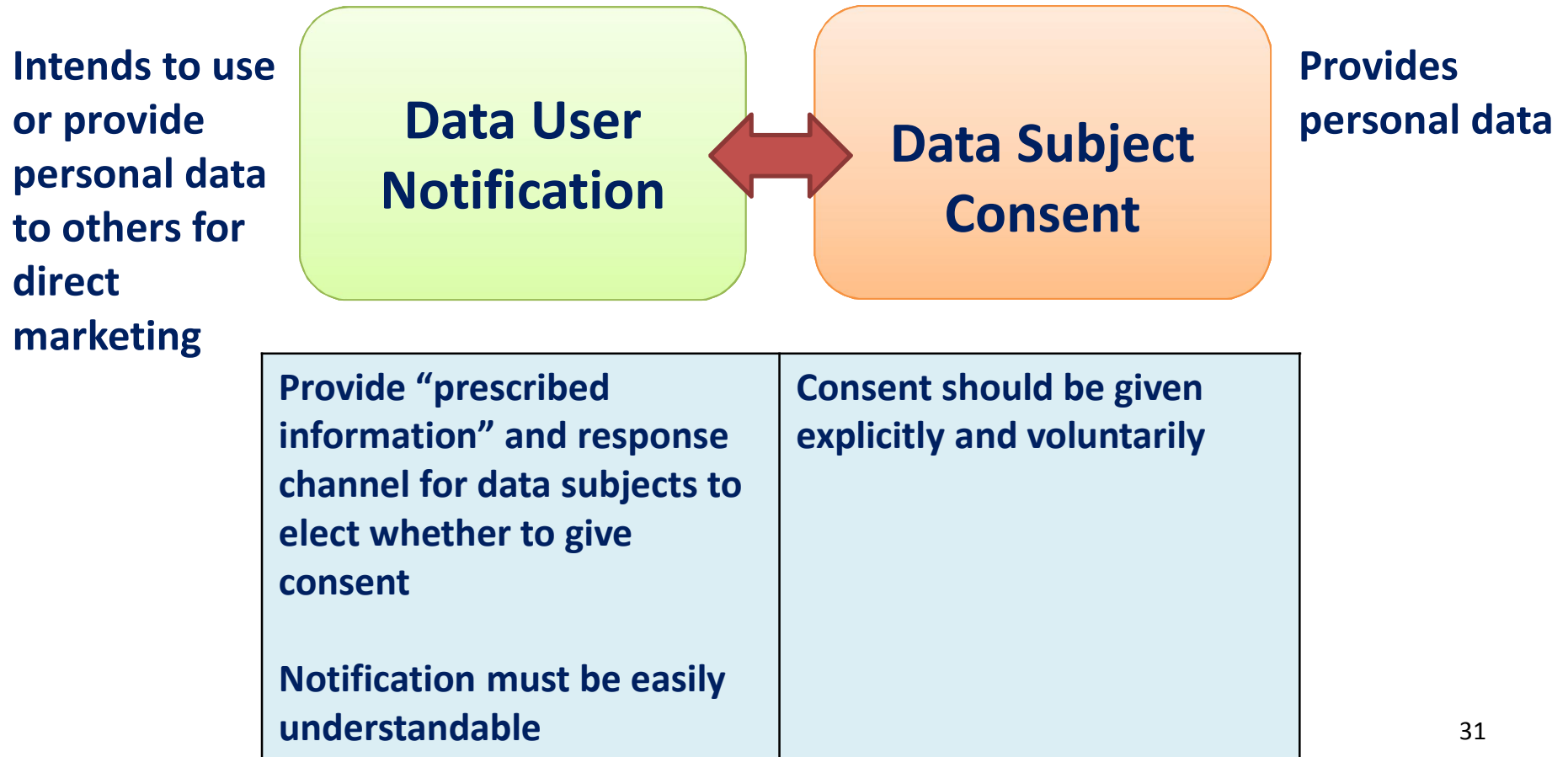
# New Direct Marketing Regime

- **Direct marketing activities under the Ordinance include such activities made to specific persons by mail, fax, email and phone**



30

# Direct Marketing Requirements



# Direct Marketing Requirements

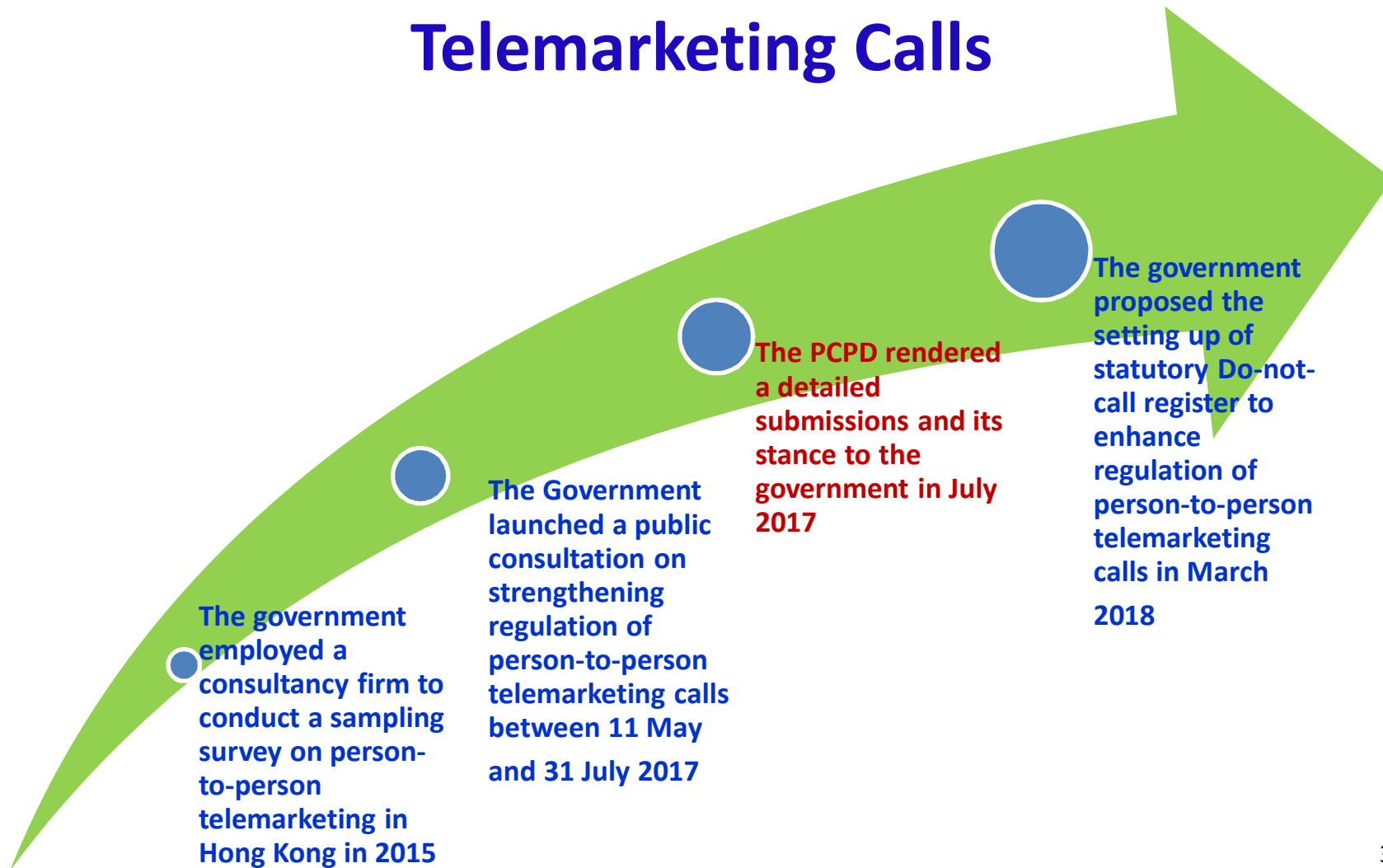
- data user must comply with the data subject's opt-out request without charge [section 35G]
- **criminal sanctions** if data user fails to comply with requirements of notification, consent and opt-out requests



32



# Regulation of Person-to-person Telemarketing Calls



# Latest Development of P2P Calls



## Set up a statutory Do-not-call register

- most effective and consumer-friendly option
- enhance regulation
- to be managed and executed by the Privacy Commissioner

34

A stylized illustration of a man with a large, dark grey mustache and a white beard. He is wearing a red and white checkered shirt. He is holding a brown telephone receiver in his right hand. The background is a light blue color with some orange circles and a white cross symbol in the upper right corner.

# Cross-border Data Transfer

# Cross-border Data Transfer

Section 33 of the PDPO prohibits transfer of personal data outside Hong Kong unless under 6 specified circumstances

Legislative intent:  
To ensure personal data transferred outside Hong Kong is afforded with same protection

# Cross-border Data Transfer

## Meaning of “Transfer”

Transfer from  
Hong Kong to a  
place outside  
Hong Kong

Transfer between 2  
other places where  
the transfer is  
controlled by a data  
user in Hong Kong

37

PCPD



H K



[PCPD.org.hk](http://PCPD.org.hk)

est.1996

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



# Cross-border Data Transfer

Data user shall not transfer personal data outside Hong Kong unless one of the conditions are met:-

s.33(2)(a)

- Fall within one of the **White List** jurisdictions (i.e. the law in that place is “*substantially similar to or serves the same purposes as*” the PDPO pursuant to PCPD’s assessment)

s.33(2)(b)

- Data user’s **own assessment** (that the law in that place is “*substantially similar to or serves the same purposes as*” the PDPO)

s.33(2)(c)

- Data subject’s **written consent** to the transfer

38

# Cross-border Data Transfer

s.33(2)(d)

- Avoidance or mitigation of **adverse action** against the data subject

s.33(2)(e)

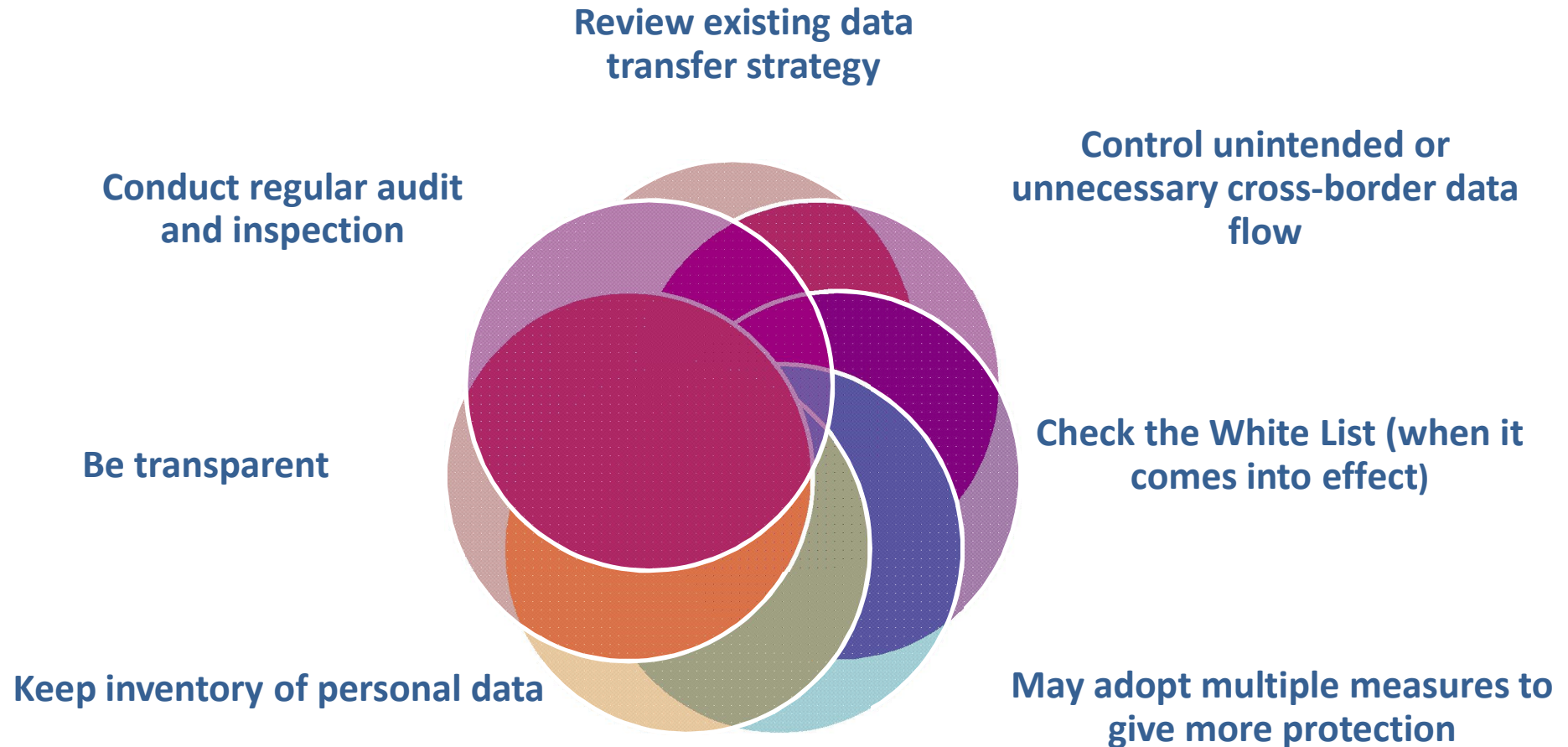
- **Exemptions** from data protection principle 3 (i.e. use limitation) under Part VIII of the PDPO apply

s.33(2)(f)

- Data user has taken **all reasonable precautions** and exercised **all due diligence** such that personal data transferred will not be handled in a manner that contravenes the PDPO (“Due Diligence Requirement”)

39

# Tips for Cross Border Data Transfer





# Guidance on Personal Data Protection in Cross-border Data Transfer

Although section 33 is not yet effective, the Guidance serves as a practical guide for data users to:

- understand compliance obligations;
- adopt the practices recommended as part of their corporate governance responsibility to protect personal data;
- consider adapting and/or including “Recommended Model Clauses” in a data transfer agreement

**指引資料**

保障個人資料：跨境資料轉移指引

第1部：引言

《個人資料(私隱)條例》(「條例」)第33條禁止將個人資料轉移至香港以外，除非符合條例列明的例外情況。該限制的目的是確保從被轉移的資料會在條例下所提供的保障。

雖然第33條尚未實施，本指引旨在為提供實惠性指引，為第33條的實施。本指引協助資料使用者了解在第33條屬於並行跨境資料轉移應遵守的禁止資料轉移的例外情況亦於本指引。

不論第33條何時生效，公眾鼓勵採取本指引內所建議的實惠行舉方式資料，作為企業管治責任的一部分。

**法律規定**

第33(2)條指明，除非符合下述其中否則資料使用者不得將個人資料轉往外的地方：

- (a) 個人資料私隱專員(「專員」)註明該地方有與條例大體上相條例的目的相同的法律。
- (b) 該使用者有合理理由相信該地方有與條例大體上相條例的目的之法律正在生效。

(需圖阿) 相信該項不列行動不屬或不是切實可行的：

Although section 33 is not yet effective, this Guidance serves as a practical guide for data users to prepare for the implementation of section 33 of the Ordinance. It helps data users to understand their compliance obligations for cross-border data transfer once section 33 is effective. All the conditions for waiving the transfer restriction are dealt with in this Guidance.

Regardless of when section 33 will take effect, data users are encouraged to adopt the practices recommended in this Guidance as part of their corporate governance responsibility to protect personal data.

**The legal requirements**

Section 33(2) specifies that a data user shall not transfer personal data to a place outside Hong Kong unless one of the following conditions is met:

- (a) The place is specified by the Privacy Commissioner for Personal Data (the “Commissioner”) by notice in the Gazette that there is in force any law which is substantially similar to, or serves the same purposes as, the Ordinance;
- (b) The data user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, the Ordinance;
- (c) The data subject has consented in writing to the transfer;
- (d) The data user has reasonable grounds for believing that the transfer is for the avoidance or mitigation of adverse action against the data subject; it is not practicable to obtain the consent in writing of the data subject to that transfer; but if it was practicable, such consent would be given;
- (e) The data is exempt from Data Protection Principle (“DPP”) 3 by virtue of an exemption under Part VIII of the Ordinance; or
- (f) The data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed, or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under the Ordinance.

PCPD  
Office of the Privacy Commissioner  
for Personal Data, Hong Kong

**Guidance Note**

Guidance on Personal Data Protection in Cross-border Data Transfer

PART 1: INTRODUCTION

Section 33 of the Personal Data (Privacy) Ordinance (the “Ordinance”) prohibits the transfer of personal data to places outside Hong Kong unless one of a number of conditions is met. The purpose of such cross-border transfer restriction is to ensure that the transferred personal data will be afforded a level of protection comparable to that under the Ordinance.

Although section 33 is not yet effective, this Guidance serves as a practical guide for data users to prepare for the implementation of section 33 of the Ordinance. It helps data users to understand their compliance obligations for cross-border data transfer once section 33 is effective. All the conditions for waiving the transfer restriction are dealt with in this Guidance.

Regardless of when section 33 will take effect, data users are encouraged to adopt the practices recommended in this Guidance as part of their corporate governance responsibility to protect personal data.

**The legal requirements**

Section 33(2) specifies that a data user shall not transfer personal data to a place outside Hong Kong unless one of the following conditions is met:

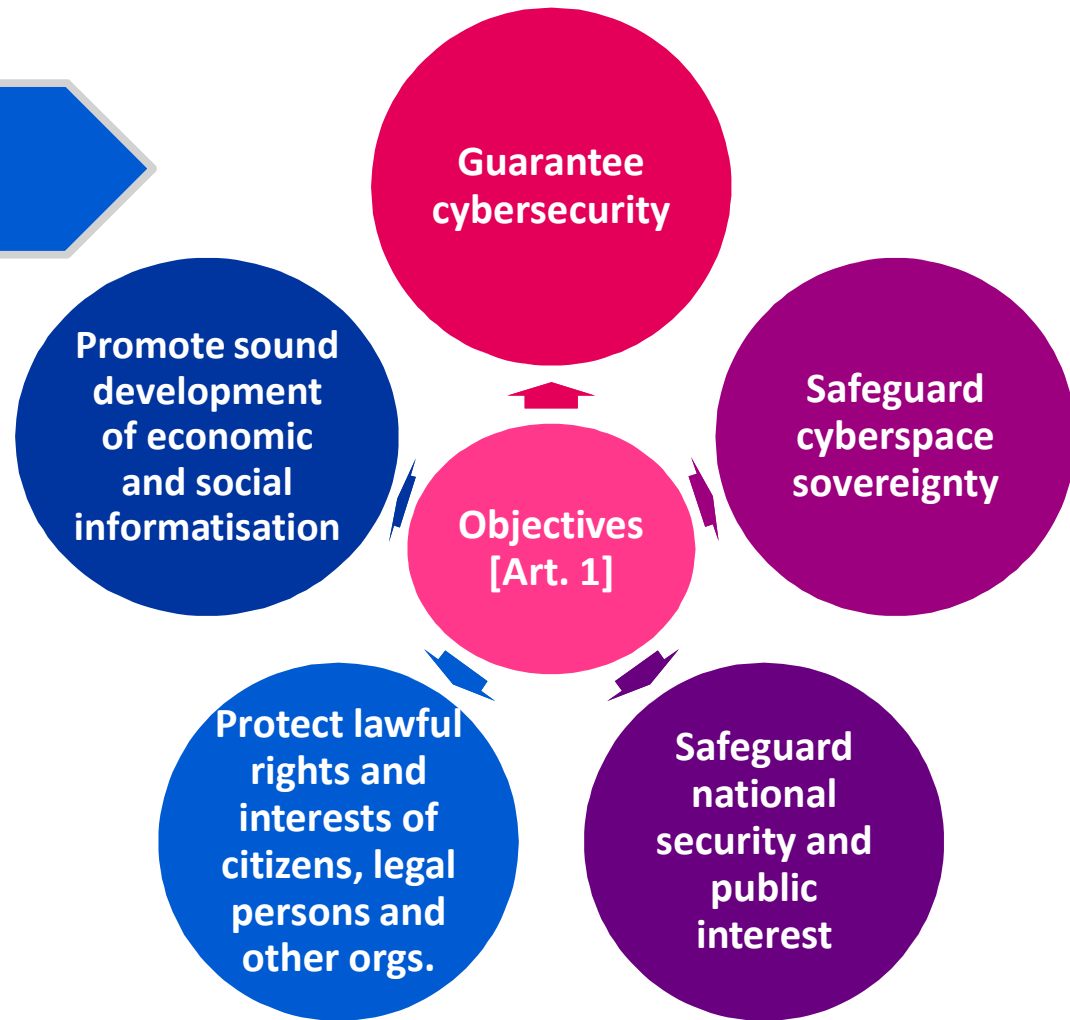
A stylized illustration of a man with a large, grey mustache and a white beard. He is wearing a red and white checkered shirt. He is holding a yellow telephone receiver to his ear. The background is a light blue color with some orange circles and a white cross symbol in the upper right corner.

# Global Data Protection Landscape - Mainland's Cybersecurity Law



# Mainland's Cybersecurity Law

- Effective on 1 June 2017
- Not apply in Hong Kong



44

PCPD



H K



PCPD.org.hk

est.1996

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

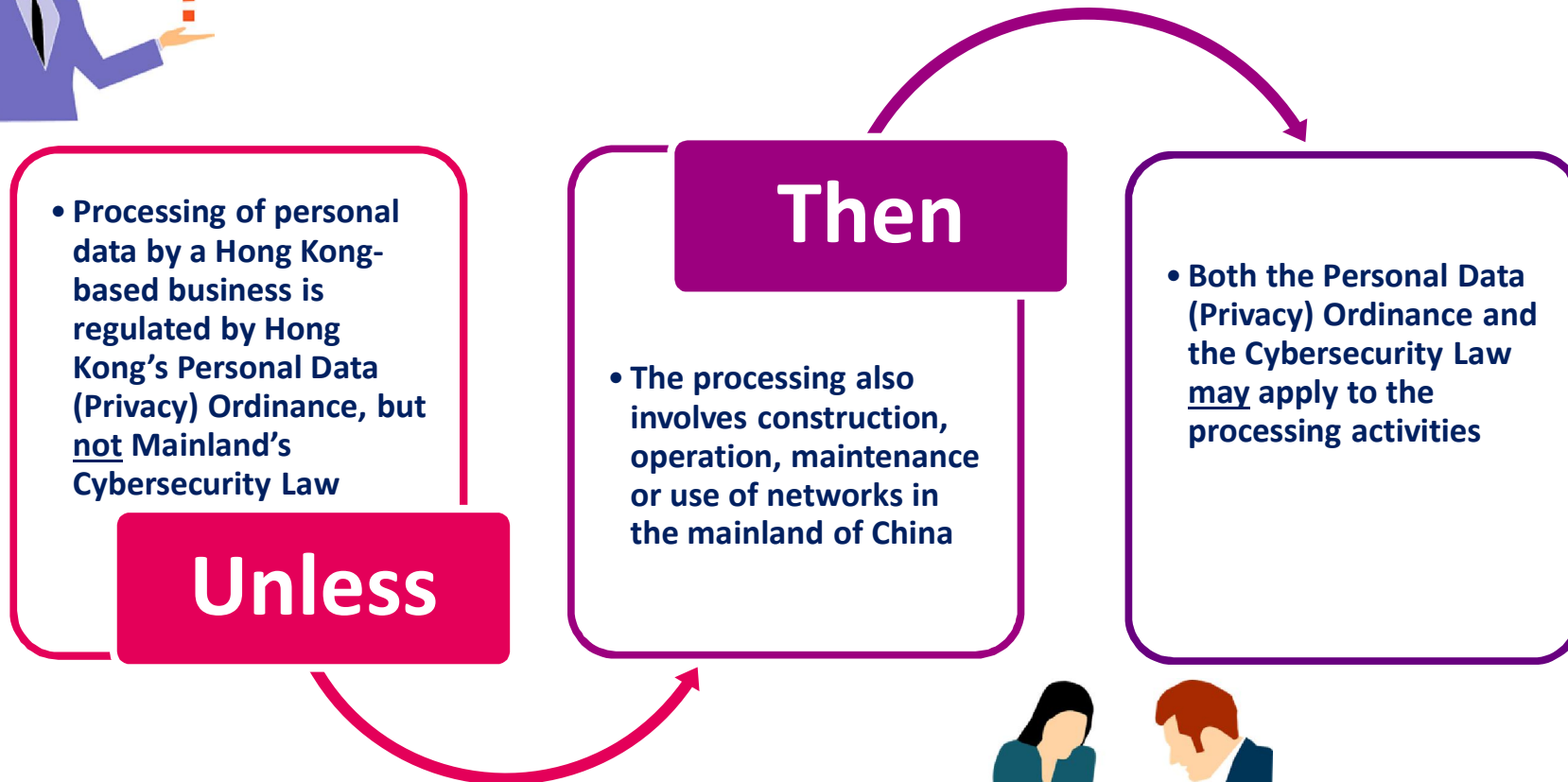
# Mainland's Cybersecurity Law

## Scope of Application:

- Apply to the construction, operation, maintenance and use of **networks**, and the supervision and administration of **cybersecurity** within China [Art. 2]
- Regulate **network operators**, i.e. owners and administrators of networks, and network service providers [Art. 76(3)]
  - Not limited to technology companies, e.g. a financial institution which uses computer network in its operation is also a 'network operator'
- Protect **personal information**

45

# How the Cybersecurity Law May Affect Hong Kong Businesses?



# Comparison between Cybersecurity Law and PDPO



## Collection & Use

Cybersecurity Law	HK PDPO
<p><u>Art. 41</u> (collection &amp; use)</p> <ul style="list-style-type: none"><li>Follow the principles of <b>lawfulness, propriety</b> and <b>necessity</b></li><li>Obtain <b>consent</b> from data subjects</li><li><b>Do not collect</b> personal information <b>irrelevant</b> to services provided</li><li>Disclose related policy and practice</li><li>Clearly indicate the <b>purposes, means</b> and <b>scope</b> of collection and use</li><li><b>Do not collect or use</b> personal information <b>in violation</b> of agreements with the data subjects</li></ul>	<p><u>DPP1</u> (collection)</p> <ul style="list-style-type: none"><li>No consent requirement</li><li>Collect data in a lawful and fair way, for a purpose directly related to a function or activity of the data user</li><li>Data collected shall be necessary but not excessive</li><li>Notify data subjects about the purpose of collection, the classes of persons to whom the data may be transferred, and the contact person</li></ul>
<p><u>Art. 42</u> (disclosure)</p> <ul style="list-style-type: none"><li>Personal information shall not be disclosed to third parties without the data subject's consent</li></ul>	<p><u>DPP3</u> (use, including disclosure)</p> <ul style="list-style-type: none"><li>Shall not use personal data for new purposes, unless with prescribed consent of data subjects</li></ul>

# Comparison between Cybersecurity Law and PDPO



## Security & Data Breach Notification

### Cybersecurity Law

#### Art. 42 (security & notification)

- Adopt **technical measures** and other measures to **ensure security** of personal information, and prevent information leakage, damage and loss
- In case of information leakage, damage or loss, take remedial actions immediately, and **notify data subjects and the supervisory authority**

### HK PDPO

#### DPP4 (security)

- Take all practicable steps to protect personal data against unauthorised or accidental access, processing, erasure, loss or use
- No requirement for data breach notification



# Comparison between Cybersecurity Law and PDPO



## Cross-border Data Transfer

### Cybersecurity Law

#### Art. 37 (data localisation)

- **Personal information** and **important data** collected and produced by operators of **critical information infrastructure** during their operations in China shall be stored locally
- If cross-border transfer is needed for business reasons, **security assessment** should be conducted pursuant to the measures stipulated by the Cyberspace Administration of China (CAC) and the relevant department of the State Council

### HK PDPO

#### S. 33 (prohibition against transfer)

- Personal data shall not be transferred to places outside Hong Kong, unless under specified circumstances, e.g.:
  - transfer to White List regions
  - consent by data subjects in writing
  - reasonable precautions taken and due diligence exercised by the data user
- S.33 is not yet in force

49

# What is Critical Information Infrastructure under Cybersecurity Law?

Examples of **Critical Information Infrastructure (CII)** under Cybersecurity Law:

- Public communications and information services
- Energy
- Transportation
- Water conservancy
- Finance
- Public services
- E-government affairs
- Other infrastructure which will cause serious damage to state security and public interests, in case of destruction, dysfunction or data leakage

[Art. 31]



50

# Comparison between Cybersecurity Law and PDPO



## Sanctions

### Cybersecurity Law

#### Arts. 64 & 66

- Possible **administrative sanctions** for a breach:
  - Corrective action
  - Warning
  - Confiscation of illegal income
  - Fine between 1 and 10 times of illegal income (if no illegal income, fine < RMB 1 million)
  - Fine between RMB 10,000 and 100,000 on directly responsible person
  - Suspension or cease of business operation for rectification, or closedown of website, or revoking of business permit or license

### HK PDPO

- PCPD has no power to impose administrative sanction

#### Ss. 50 & 50A

- The Privacy Commissioner may issue an enforcement notice, ordering remedial actions by a data user
- Non-compliance with an enforcement notice may (upon conviction by a court) subject to a fine of HK\$50,000 and imprisonment for 2 years

51

A stylized illustration of a man with a large, light-colored beard and a dark mustache. He is wearing a red and white checkered shirt. He is holding a yellow telephone receiver to his ear. The background is a light blue gradient with some orange circular shapes in the upper right corner.

# **How to Nurture an Organisational Cultural of Respecting Personal Data Privacy**

# Privacy Management Programme

**From Compliance**  
*to Accountability*



# What is PMP?

## Paradigm Shift

Compliance Approach	Accountability Approach
<ul style="list-style-type: none"><li>• <b>passive</b></li><li>• <b>reactive</b></li><li>• <b>remedial</b></li><li>• <b>problem-based</b></li><li>• <b>handled by compliance team</b></li><li>• <b>minimum legal requirement</b></li><li>• <b>bottom-up</b></li></ul>	<ul style="list-style-type: none"><li>• <b>active</b></li><li>• <b>proactive</b></li><li>• <b>preventive</b></li><li>• <b>based on customer expectation</b></li><li>• <b>directed by top-management</b></li><li>• <b>reputation building</b></li><li>• <b>top-down</b></li></ul>

# Participation in the PMP

## Pledging Organisations

- ✓ 76 bureaux and departments of Hong Kong Government
- ✓ 25 Insurance companies
- ✓ 9 Telecommunication companies
- ✓ 5 Organisations from other sectors

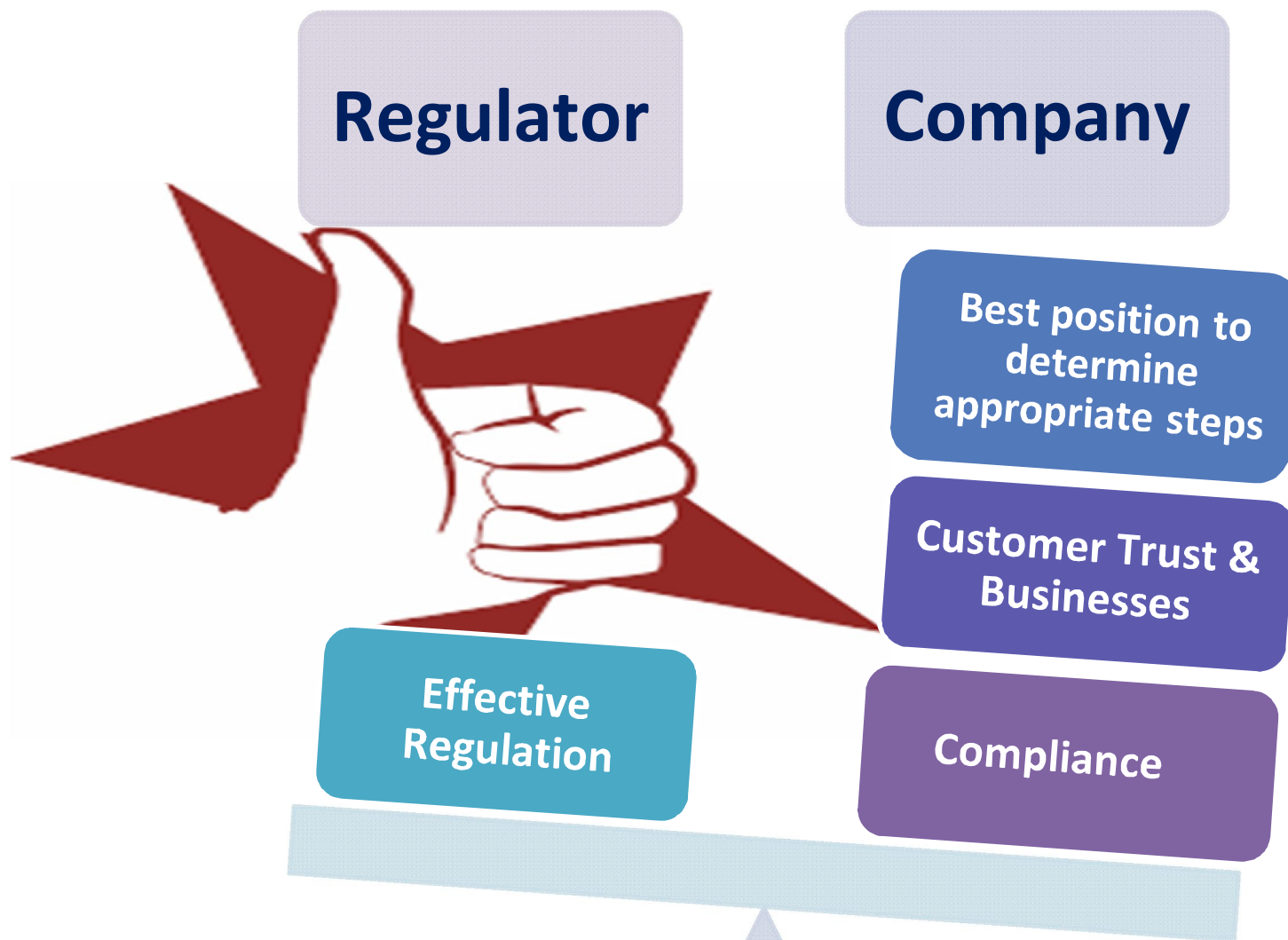




A stylized illustration of a man with a large, grey, bushy mustache and a white beard. He has a neutral expression with small black eyes and a simple white mouth. He is wearing a red and white checkered shirt. In his right hand, he holds a brown telephone receiver with a coiled cord. The background is a light blue gradient. In the upper right corner, there are several orange circles of varying sizes, some with white plus signs, suggesting a thought bubble or a list of items.

# Ethics & Accountability

# Why Accountability?



# Mechanics of Accountability

Voluntary/Self-Regulatory  
or  
Mandatory  
Accountability?

Education → Incentivise



58



# Data Ethics and Trust



- No Surprise to Consumers
- No Harm to Consumers

A stylized illustration of a man's face and upper torso. The man has a large, light-colored head with a dark mustache and a small white mustache above it. He is wearing a red and white checkered shirt. He is holding a brown telephone receiver to his ear with his right hand. The background is a light blue color with some orange circles and a white cross symbol in the upper right corner.

# Case Sharing

# Direct Marketing – Conviction Case 1

## ● First Conviction Case – Case background

- A customer of a telecommunications company made his opt-out request to the Company via email and mail
- The Company acknowledged receipt of the complainant's opt-out request in writing
- A staff member of the Company left a voice message through the customer's mobile phone number, informing him the termination of his service contract and at the same time promoting their services to him

## ● Outcome

- The Company was fined HK\$30,000

61

## Direct Marketing – Conviction Case 2

- personal data in the online Government Telephone Directory for direct marketing



**CONVICTED**



62



# Claims made under Section 66 of the PDPO (DCCJ 3793/2016)

- Section 66 of the PDPO provides that an individual who suffers damage by reason of a contravention of a requirement under the PDPO by a data user may be entitled to compensation from that data user for that damage. The Privacy Commissioner may, pursuant to section 66B of the PDPO, grant legal assistance to the aggrieved individual who intends to institute proceedings to seek compensation.
- **Brief Facts of the Case**
  - The Plaintiff lodged her complaint with PCPD against an organisation for disclosure of case materials of a criminal charge laid against her
  - The Plaintiff appealed to the Administrative Appeals Board against PCPD's decision not to proceed with her complaint, but her appeal was dismissed
  - The Plaintiff commenced an action in the District Court to claim damages for contravention of DPP3 and DPP4
  - The Defendants applied to the District Court for striking out the Plaintiff's claims

63



# Claims made under Section 66 of the PDPO (Con't)

## (DCCJ 3793/2016)

- **Gist of Court's Ruling**

- The Board has jurisdiction over the subject matter, and its decision is conclusive and final
- The issues determined by the Board are identical to those presented to the District Court. The parties are also the same
- Balancing against the oppression that would be caused to the Defendants in the present proceedings, the District Court ordered the Plaintiff's claims be struck out on the ground that the common law principle of "res judicata" applied

- **Significance**

- Implications on PCPD's handling of legal assistance cases
- Should the Board find the defendant to have contravened any requirement of the PDPO, the defendant will not be allowed to challenge the question of liability in his civil claim for damages

64

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

歐洲聯盟  
《通用數據保障條例 2016》  
小冊子 – 中文版



歐洲聯盟  
《通用數據保障條例 2016》  
小冊子 – 英文版



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

[PCPD.org.hk](http://PCPD.org.hk)



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