The Hong Kong Polytechnic University: MSc in Tourism Marketing
The Professor of A Day –

Data Privacy - the Law and Ethics

3 April 2020 | Polytechnic University, Hong Kong

Stephen Kai-yi WONG, Barrister
Privacy Commissioner for Personal Data, Hong Kong, China

Multiple data security incidents involving travel agencies in 2017 - 2018

2020年3月11日 星期三 5:15PM
19°C

明報新聞網

主頁 | 每日明報 | 即時新聞 | 明報OL網 | 明報影片 | 明報健康

要聞 | 港聞 | 經濟 | 娛樂 | 社評 | 觀點 | 中國 | 國際 | 教育 | 體育 | 副刊 | 英文 | 作家專欄 | 創科線

熱門話題：抗疫新階段，曹星如，謝振中，習近平，特朗普，郭蓬庶，歐聯，張栢芝，獸醫教用漂白水

港聞 港聞二

2018年1月4日星期四

大航假期遭黑客勒索 部分客個人資料被盜

上一篇 下一篇

大航假期遭黑客勒索 部分客個人資料被盜

讚好 0

【明報專訊】繼去年縱橫遊被黑客入侵，20萬客戶資料外泄後，大航假期前日（2日）亦接獲黑客勒索信息，表示已持有該公司部分客戶的個人資料，包括姓名、身分證及回鄉證等，但不涉信用卡。警方網絡安全及科技罪案調查科已接手跟進，個人資料私隱專員公署亦展開循規審查。

信報 HK STARTUPS 融資紀錄 人工智能 FINTECH 生物科技

縱橫遊遭黑客入侵勒索 系統被封資料外洩 分行今午重開

By 信報財經新聞 on November 8, 2017

Like Sign Up to see what your friends like.

原文刊於信報

縱橫遊昨天全線分行停業，電話報名中心則照常營運。（nowTV截圖）

擁有38年歷史的縱橫遊旅行社疑遭黑客入侵電腦系統，其母公司縱橫遊控股（08069）昨天傍晚發聲明表示，發現有未經授權人士於11月6日存取系統內的客戶數據庫，之後收到電郵勒索，要求贖金以解除系統封鎖，公司已即時報警，案件由網絡安全及科技罪案調查科接手。昨日縱橫遊全線分行停業，於今天（8日）中午起恢復有限度服務，而電話

now 新聞

直播 港聞 兩岸國際 娛樂 生活 科技 財經 體育

金怡假期遭黑客入侵 外洩資料涉身份證及電話號碼

金怡假期遭黑客入侵 外洩資料涉身份證及電話號碼

2018年1月4日 21:56

【Now新聞台】再有旅行社懷疑遭黑客入侵，金怡假期伺服器懷疑被黑客攻擊，公司已報警處理。負責人表示，今次被洩漏的客戶資料涉及身份證、電話號碼等，但不包括銀行及信用卡資料。警方會將金怡假期及大航假期遭黑客入侵的個案合併調查。

廣告

熱門新聞

1 【持續更新】香

South China Morning Post SIGN IN/UP

Hong Kong / Transport

Personal data of 9.4 million passengers of Cathay Pacific and subsidiary leaked, airlines say

- Information consists of passengers' names, nationalities, dates of birth, identity card numbers and historical travel details
- Suspicious activity detected in March, prompting a cybersecurity investigation – but IT lawmaker questions why carrier waited till now to disclose breach

Danny Mok
Published: 11:53pm, 24 Oct, 2018

1.2k

Significant data breach in 2018 of a Hong Kong based airline

Source: https://www.scmp.com/news/hong-kong/transport/article/2170076/personal-data-some-94-million-passengers-cathay-pacific-and

Significant data breach incidents in International Hotel Franchises in 2016 and 2018

The Washington Post
Democracy Dies in Darkness

Business

Marriott discloses massive data breach affecting up to 500 million guests

Marriott International said on Nov. 30 its Starwood Hotels brand's reservation database was breached by an unauthorized party that had access since 2014. (Reuters)

By **Taylor Telford** and **Craig Timberg**

Dec. 1, 2018 at 2:03 a.m. GMT+8

Source: https://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/

TREND MICRO

Unternehmen › Privatanwender ›

Produkte IoT-Sicherheit Informationen Support Partner Über uns

Kontakt

Nachrichten zum Thema Sicherheit › Cyber Attacks › 250 Hyatt Hotels Across 50 Countries Hit by Data Breach

250 Hyatt Hotels Across 50 Countries Hit by Data Breach

15 Januar 2016

Last Thursday, Hyatt announced that it discovered malicious software in about 250 of its hotels' payment processing systems (mainly at its restaurants) that may have compromised customers' credit and debit card details. According to Hyatt, the malware was present from August 13 to December 8, 2015.

Web Skimming Attack on Blue Bear Affects School Admin Software Users

Drilling Deep: A

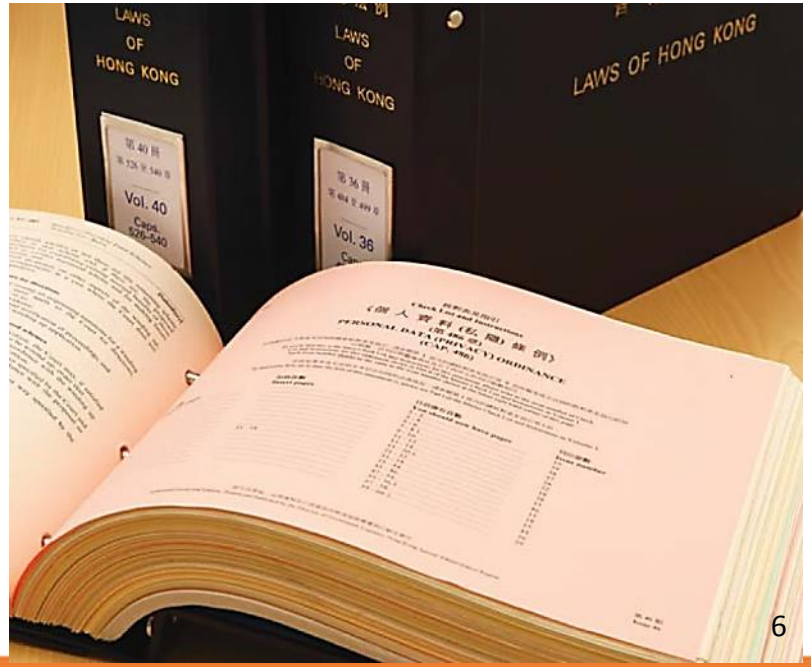
Source: https://www.trendmicro.com/vinfo/de/security/news/cyber-attacks/250-hyatt-hotels-across-50-countries-hit-by-data-breach

Personal data belongs to individuals

…how can personal data be better protected?

Personal Data (Privacy) Ordinance
Cap 486, Laws of Hong Kong

- Enacted in 1995
- Protects individuals' privacy in relation to personal data
- Created an independent Privacy Commissioner for Personal Data
- Covers the public (including the government) and private sectors
- Referenced to 1980 OECD Privacy Guidelines and 1995 EU Data Protection Directive



Six Data Protection Principles (DPPs) of the PDPO

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.

2 準確性、儲存及保留 Accuracy & Retention

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

Practicable steps shall be taken to ensure personal data is accurate and not kept longer than is necessary to fulfil the purpose for which it is used.

3 使用 Use

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

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

4 保安措施 Security

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

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

5 透明度 Openness

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

A data user must take practicable steps to make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used.

6 查閱及更正 Data Access & Correction

資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

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

Amendments in 2012 – Strengthened Regulation on Direct Marketing

- **Provide prescribed information** to individuals (e.g. kinds of personal data to be used, types of goods & services)
- Obtain individuals' **consent**
- Allow individuals to **opt out**
- Maximum penalties for contravention: **fine of HK$1 million + imprisonment for 5 years**

International and local developments

The EU implemented GDPR in May 2018

High-profile data breaches in Hong Kong in recent years (e.g. CX, HKBN, REO, TransUnion, doxxing)

Ever-evolving technological landscape

Call for PDPO reform is loud

The Government presented amendment directions for the PDPO to Legislative Council in January 2020:

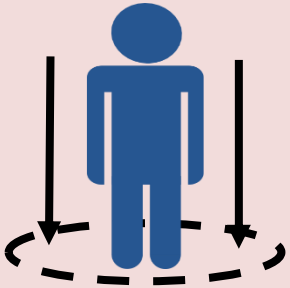
- ❑ Mandatory data breach notification mechanism
- ❑ Requirements on setting out data retention policy
- ❑ Empowering PCPD to impose administrative fines and increasing the level of criminal fines
- ❑ Regulating data processors
- ❑ Expanding the definition of ‘personal data’
- ❑ Regulating doxxing

TRENDS IN TOURISM MARKETING

Online Booking Platforms

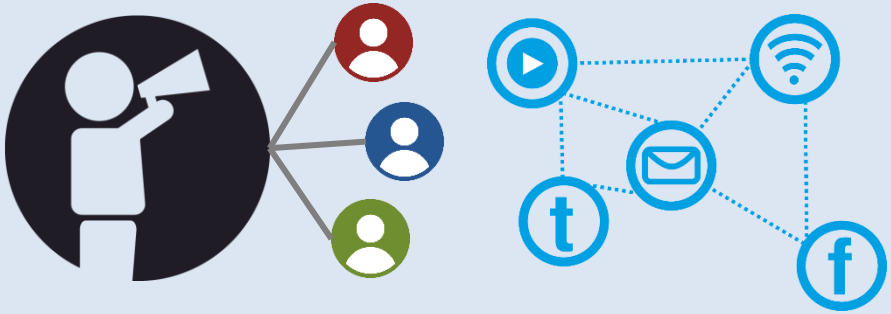
Use of AI, Robots, Chatbots to provide services

Facial Recognition Kiosk for Check-in



Personalised recommendations

Review Marketing



Influencer Marketing on Social Media

TRENDS IN TOURISM MARKETING

Remarketing

Virtual Reality & Augmented Reality

Challenges in Tourism Marketing

DATA SECURITY

More data about customers is collected

The industry possesses a treasure trove of personal data-

- **Name, passport number, credit card number, travel history, location data**.

And more activities have ***gone online***

Information systems are not as strong as those of the banking and healthcare industries, and many of them may be legacy systems which are **susceptible to hacking**.

TRANSPARENCY OF PRIVACY PRACTICE

- What **kinds of personal data** are collected by websites, service robots, and chatbots?
- What are the **intended uses** of the collected personal data?
- Who/what are the **potential transferees** of the personal data collected?

Challenges in Tourism Marketing

CUSTOMERS' CHOICES AND CONTROL

Innovative technology replaces traditional ways of service in the industry, e.g.-

- facial recognition check-in;
- personalised ads and recommendations

Always provide customers a choice:

→ The choice to use less privacy-intrusive alternatives

→ The option to opt-out from personalised services

COMPLIANCE WITH DIRECT MARKETING REQUIREMENTS

For Remarketing, i.e. targeting those who have interacted with your business in the past-

- Personal data may have been collected for non-marketing purposes
- **Consent must be obtained** for personal data to be used for remarketing purposes
- The **option to opt-out** must be provided

Challenges in Tourism Marketing

ETHICAL CONCERNS

Price discrimination-

- Enabled by collecting data about the consumers, e.g. via cookies on websites
- According to research, **over 80% of consumers feel they have lost all control** over how their personal information is collected and used by companies (Source: J.D. Power)
- Could be considered unethical if data was collected to adjust prices, and customers' trust could be lost
- E.g. "大數據殺熟"

人民网 people.cn 人民网 >> 河南频道

大數據"殺熟"調查：越是老顧客越給你優惠越少

2018年04月24日07:47 來源：人民網-人民日報 分享到：

原標題：人民日報談大數據"殺熟"：上網享便利 消費防算計

上網享便利 消費防算計(一線調查·互聯網新觀察續⑦)

核心閱讀

多家網絡電商平台近期被曝出存在大數據"殺熟"行為，即老客戶購買某種產品或服務反而比新客戶花錢更多。大數據"殺熟"現象，是否真的存在？"殺熟"侵犯了消費者哪些權益？怎樣才能在產業發展和消費者維權之間做出平衡？對此，記者展開調查。

平台背信——

■既不符合道德要求，也違反法律規定

熱點推薦

人民日報：鼓勵揭短
三大城市的"引才答
人民日報評馬拉松扎
河南駁羽六項紀律處
全國首家村級黨員政
戊戌年黃帝故裡拜祖
完善醫養結合模式
曹衛洲：推動"國際
鄭州非機動車管理辦
二類疫苗打不打、怎

Source: http://henan.people.com.cn/BIG5/n2/2018/0424/c351638-31498196.html

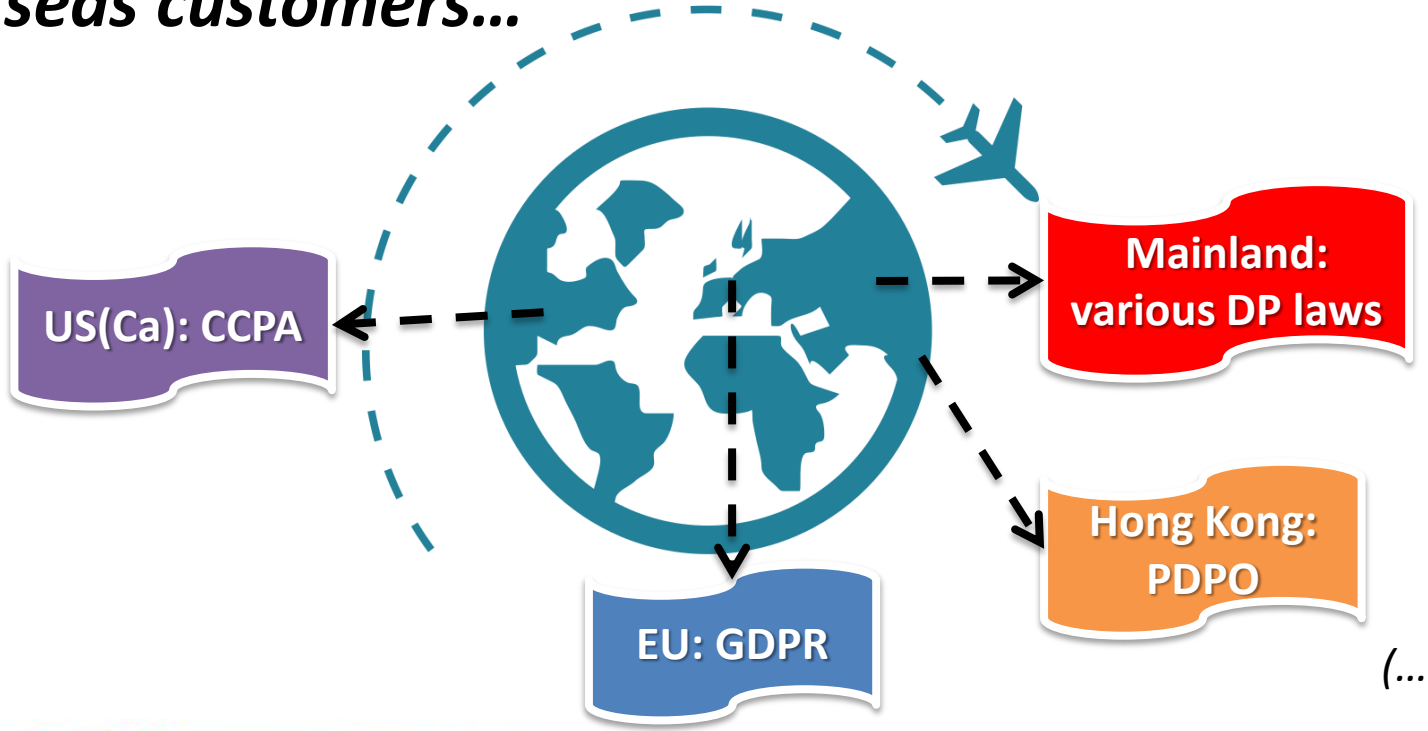
Challenges in Tourism Marketing

TRUSTWORTHINESS

Review Marketing & Influencer Marketing-

- Consumers, especially millennial consumers, view that **consumer-generated content are more trustworthy** than traditional advertisements placed by brands
- 63% of consumers trust influencers over brands (Source: Edelman)
- **Issue of credibility** with online reviews and influencers' reviews: online content may be **easy to fabricate**

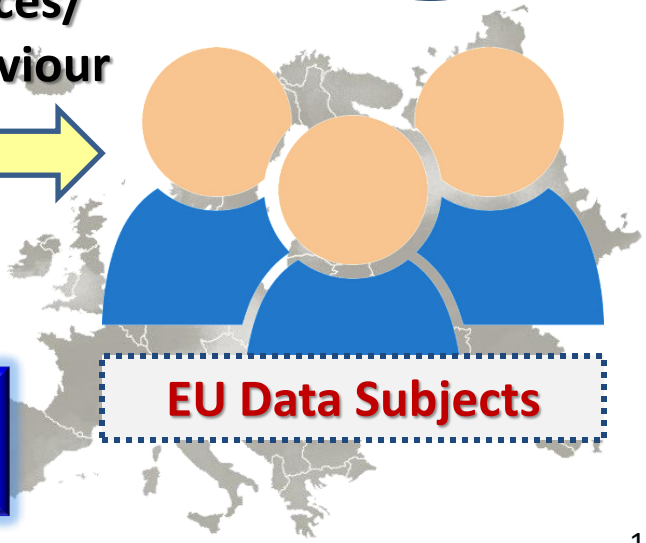
The tourism and hospitality industry offers services to overseas customers…



(…and more)

Implemented: May 2018

Offer goods & services/
Monitor online behaviour



International businesses in Hong Kong (even with no establishments in the EU)

Extraterritorial effect: ✓ GDPR APPLIES

EU Data Subjects

California Consumer Privacy Act (CCPA)

Implemented: Jan 2020

International businesses in Hong Kong (even with no establishments in California)

Doing business in California

Extraterritorial effect:
✓ CCPA APPLIES

Mainland of China - Cybersecurity Law

Came into force in June 2017

Data localisation requirements for personal information and important data collected by operators of "critical information infrastructure" (CII) **[Articles 31 and 37]**

- "CII": e.g. financial, energy, telecom and information services, water, transportation, public services, e-government and other key industries;
- **Security assessment** is needed if there is a real necessity to **transfer out of mainland China for business purposes**

Measures for Security Assessment for Cross-border Transfer of Personal Information (Consultation Draft)

Issued by the **Cyberspace Administration** of China in June 2019

Legally binding when it comes into force

Provides for **requirements on security assessment** under Cybersecurity Law article 37

Extends the requirements on security assessment to all network operators (vs. CII operators under Cybersecurity Law)

Extra-territoriality:

Apply to: Organisations located outside the mainland of China collecting personal information of users in the mainland of China via the internet or other means

Requirements: Fulfil obligations under the Measures through their legal representatives in the mainland of China

How may Cybersecurity Law affect Hong Kong businesses?

- Processing of personal data by a Hong Kong-based business is regulated by Hong Kong's Personal Data (Privacy) Ordinance, but <u>not</u> Mainland's Cybersecurity Law

Unless

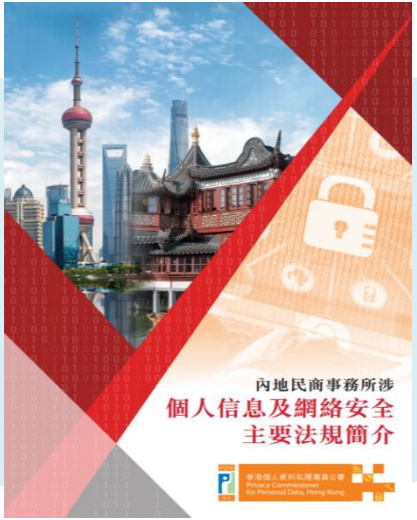
Then

- The processing also involves construction, operation, maintenance or use of networks in the mainland of China

- Both the Personal Data (Privacy) Ordinance and the Cybersecurity Law <u>may</u> apply to the processing activities

- CLC has no explicit extraterritoriality
- But be wary of collecting personal information from individuals in mainland

Relevant PCPD publications



Booklet: 'Introduction to the Regulations in the Mainland of China Concerning Personal Information and Cybersecurity Involved in Civil and Commercial Affairs'

Booklet: '*European Union General Data Protection Regulation 2016*'

Case study:

Data breach of an airline based in HK affecting 9.4m passengers

Background

- Suspicious activities on its network detected in March 2018
- Data breach notification lodged to PCPD on 24 Oct 2018
- 9.4 million passengers from over 260 countries / jurisdictions / locations affected
- Personal data involved consisted mainly of name, flight number and date, email address, membership number, address, phone number

Case study:

Data breach of an airline based in HK (cont.)

PCPD's investigation and findings

Investigation focuses

- DPP4: Data security
- DPP2: Data retention period

Contraventions

- Various data security failures (see following slides)
- Not taking all reasonably practicable steps to erase unnecessary HK Identity Card No. of passengers

Case study:

Data breach of an airline based in HK (cont.)

PCPD Enforcement Notice issued

Date security failures include:

- Risk alertness being low — Corporate governance failure
- Vulnerability scanning exercise at a yearly interval (too lax) — Risk assessment failure
- Failure to identify and address the commonly known exploitable vulnerability — Technical measure failure
- Failure to have an effective personal data inventory — Operational measure failure
- Failure to apply effective multi-factor authentication to all remote access users

Case study:

Data breach of an airline based in HK (cont.)

BBC News Sport Reel Worklife Travel More Search

NEWS

Home Video World Asia UK Business Tech Science Stories More

Technology

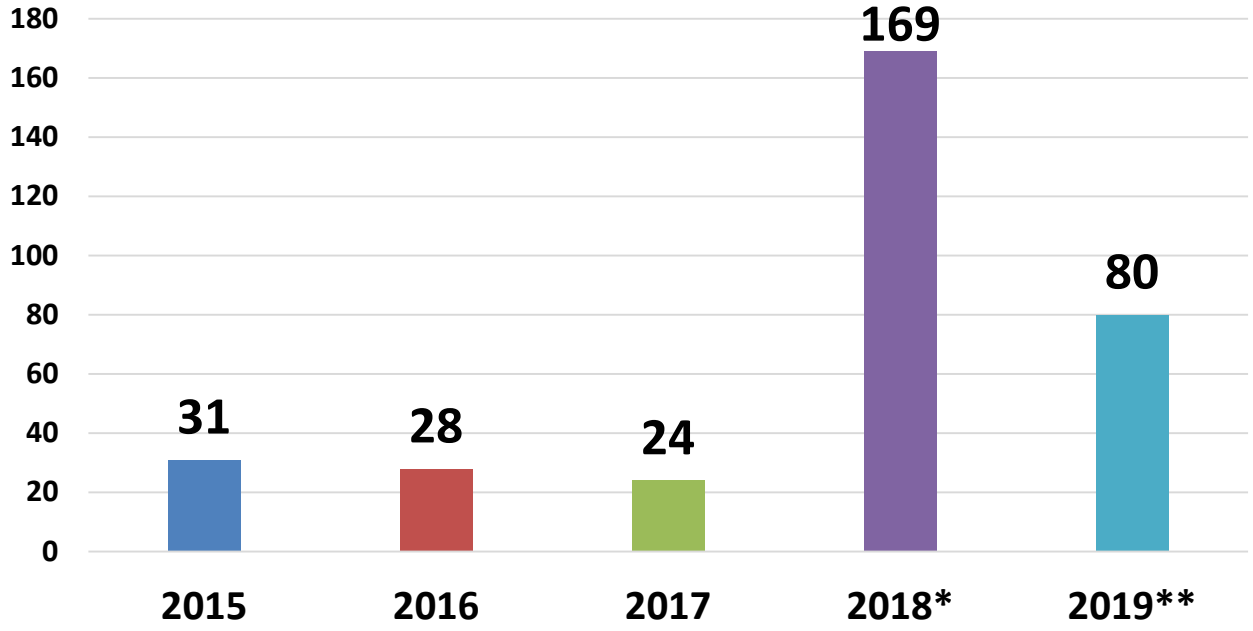
Cathay Pacific fined £500,000 over customer data protection failure

4 March 2020 Share

The UK **Information Commissioner's Office (ICO)** imposed the maximum pre-GDPR financial penalty **£500,000** on the airline in Feb 2020 for failing to protect customers' personal data as over 111,000 Britons were affected.

Source: https://www.bbc.com/news/technology-51736857

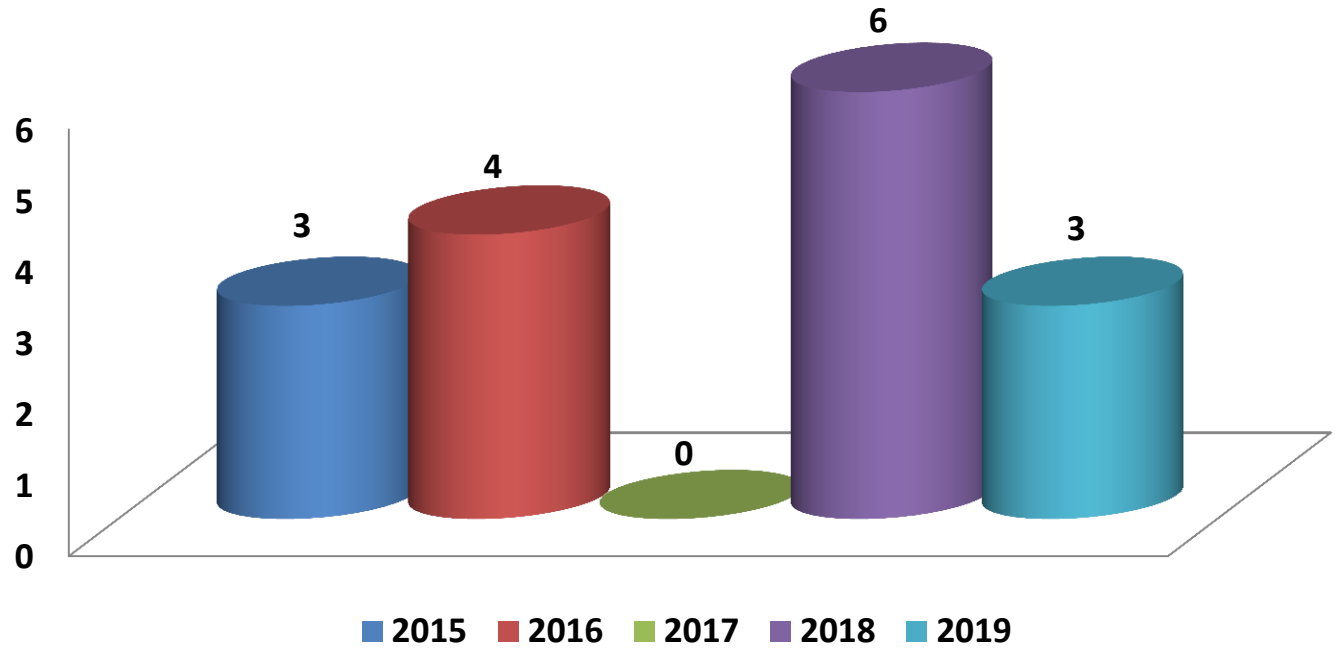
No. of Complaints received against Travel agencies, Airlines, Hotels, Travel websites



*: includes 139 complaints related to the incident of leakage of passengers' personal data by Cathay Pacific Airways.

**: includes 41 complaints related to the suspected online disclosure of flight information concerning "HK Police Football" by a staff member of Cathay Pacific Airways.

Data Breach Notifications received from Travel agencies, Airlines, Hotels, Travel websites



How may the industry improve their practices?

In PCPD's **inspection report** on a **travel agent** published in Jan 2016-

Background

- Travelling abroad is a favourite pastime in Hong Kong
- Over 1,700 licensed travel agents in Hong Kong
- Vast amount of customers' personal data are collected and retained by travel agents (e.g. name, passport details, date of birth, contact information, and credit card details)
- An inspection of the travel agent's personal data system could help promote compliance in the industry

How may the industry improve their practices? (cont.)

In PCPD's **inspection report** on a **travel agent** published in Jan 2016 (cont.)-

Minimise collection of personal data

- Is there a need to collect the address and HKID card number from a tour customer who **books a tour online**?
- Is there a need to collect full D.O.B. from **loyalty programme** members to process the membership application and the points earning/redemption?

Transparency

- Devise a **privacy policy statement** and make it available online.
- Specify precisely the classes of persons to whom tour customers' personal data may be transferred.
- Specify that there is no transfer of loyalty programme members' personal data to any other parties, if that is the case.

How may the industry improve their practices? (cont.)

In PCPD's **inspection report** on a **travel agent** published in Jan 2016 (cont.)-

Direct Marketing Practices

- **Relocate the tick box** on the paper registration form (for customers to indicate objection to the use of their personal data in direct marketing) to **a more prominent place.**

Data Security Measures

- Formally **document the administrative measures** to safeguard the sensitive documents in transit.
- Fully **encrypt personal data** transmitting through the internet.
- Review and improve the existing **IT security policy and IT governance** to ensure its comprehensiveness and integrity
- Improve the **data breach handling guideline.**

There are some examples of good practices too!

- ✓ Commitment to privacy management by **assigning a high-ranking management officer** to oversee privacy matters;
- ✓ **Only necessary data is collected** from a customer when tour services are **booked at a branch**;
- ✓ **Timely destruction** of documents containing personal data
- ✓ **Secure handling** of sensitive documents

Accountability

Responsibility to put in place adequate policies and measures to ensure and demonstrate compliance

Rationale: Data users are in the best position to identify, assess and address the privacy risks of their activities

PCPD's Accountability Framework: Privacy Management Programme (PMP)

- **Voluntary accountability framework**
- **First published – February 2014**
- **First revision – August 2018**
- **Pledged organisations:**
  - **All government bureaus and departments**
  - **37 commercial and public organisations** (e.g. insurance, telecommunications, transportation, heath care, public utilities)
- **PMP Manual for private sector published in 2019**

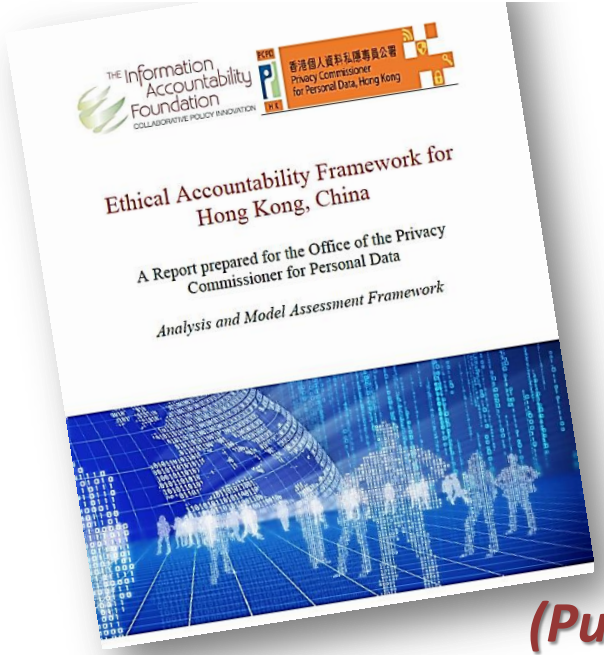
PCPD's Accountability Framework:

Privacy Management Programme (PMP)

https://www.pcpd.org.hk/pmp/index.html

- Effective management of personal data
- Minimisation of privacy risks
- Effective handling of data breach incidents
- **Demonstrate compliance and accountability**

“Ethical Accountability Framework for Hong Kong, China”



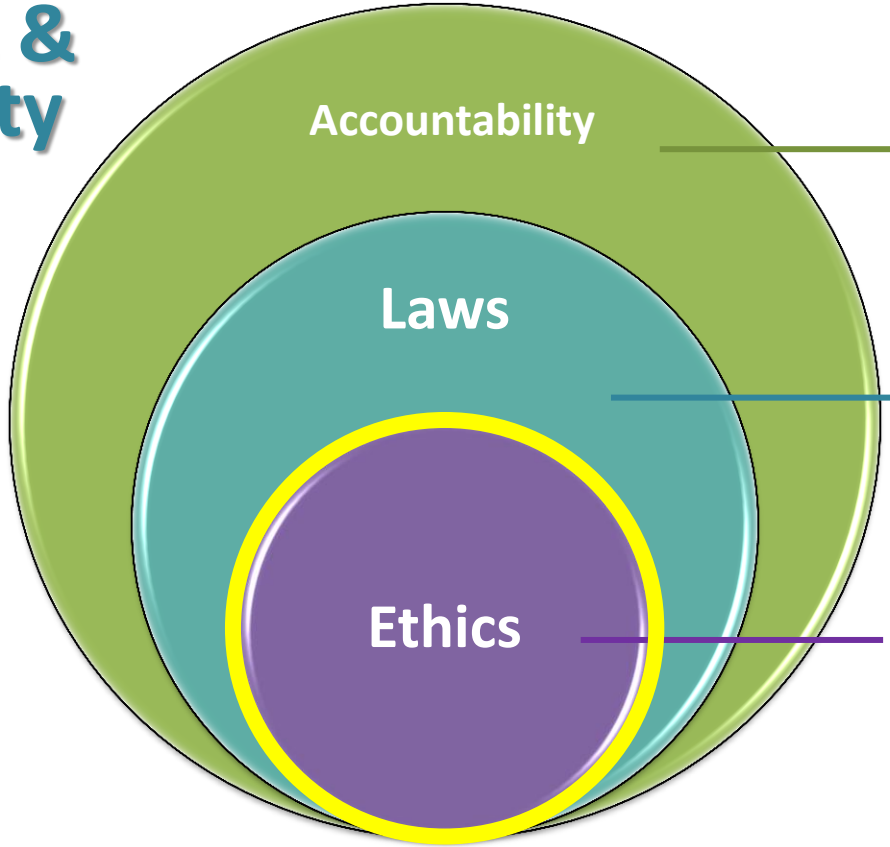
In collaboration with:

THE Information Accountability Foundation
COLLABORATIVE POLICY INNOVATION

(Published on 24 October 2018)

Download >>

Ethics, Laws, & Accountability

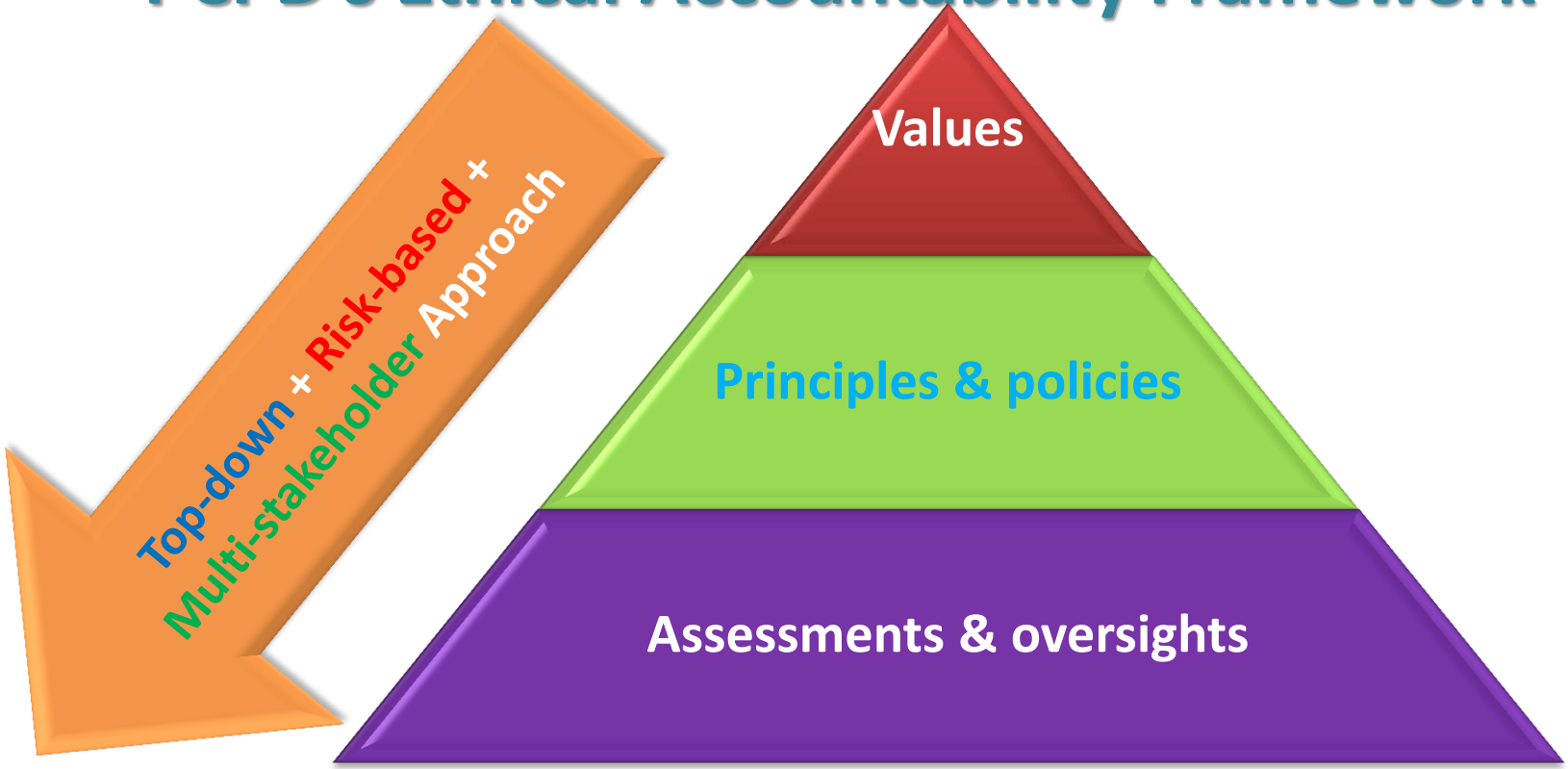


Extended obligation to ensure compliance with laws

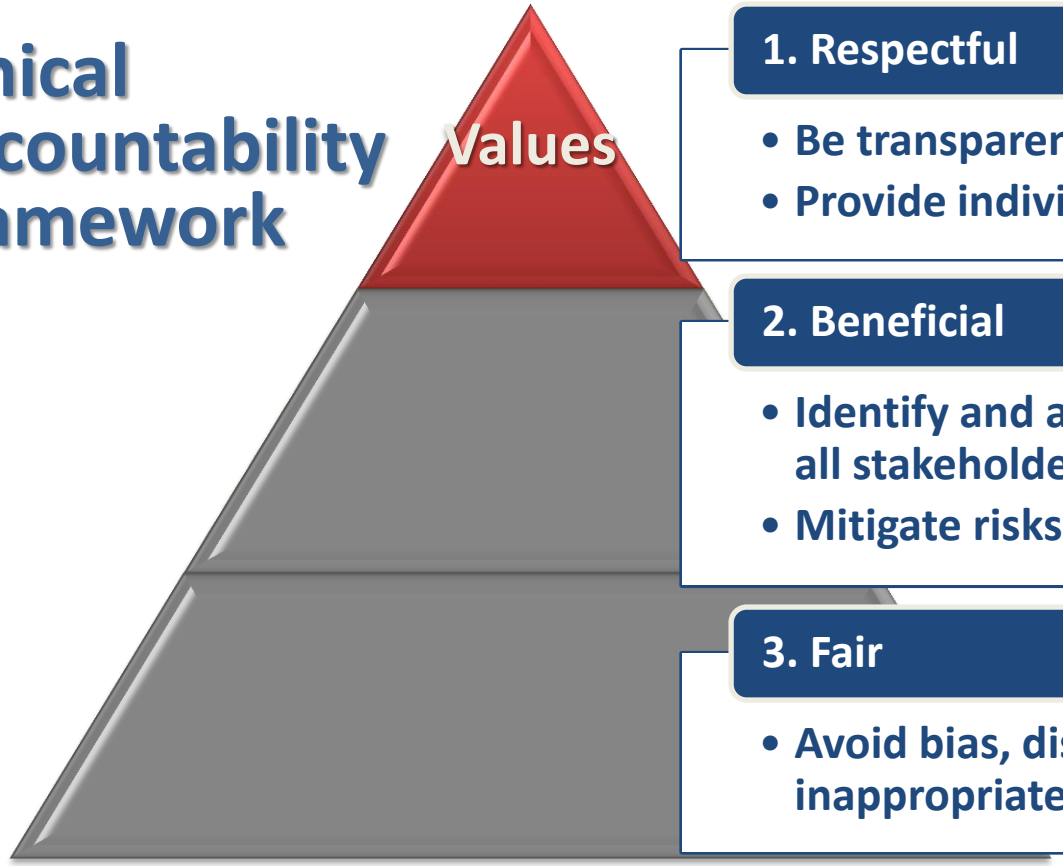
Legal obligations, usually based on communal values

Communal values shared by the public in general, guiding our daily living

PCPD's Ethical Accountability Framework



Ethical Accountability Framework



1. Respectful

- Be transparent
- Provide individuals with control

2. Beneficial

- Identify and assess risks and benefits to all stakeholders
- Mitigate risks

3. Fair

- Avoid bias, discrimination and other inappropriate actions

HKMA's circular on 3 May 2019

- To all authorized institutions
- Encourages them to adopt and implement the PCPD's *'Ethical Accountability Framework'* in the development of fintech products and services

https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2019/20190503e1.pdf

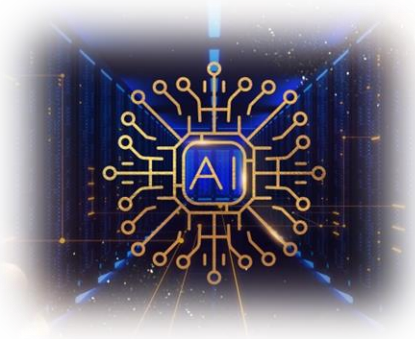
HKMA's four '*Guiding Principles on Consumer Protection in respect of Use of Big Data and AI*' (Issued Nov 2019)

1. Governance and Accountability
2. Fairness
3. Transparency and Disclosure
4. Data Privacy and Protection

Informed/Inspired by PCPD's '*Ethical Accountability Framework*'

Some banks developing their own principles, taking reference from those of PCPD and HKMA

PCPD co-chairs the **GPA Working Group on Ethics and Data Protection in Artificial Intelligence**



GPA
Global Privacy Assembly

Why is ethics so important?

Edelman Trust Barometer 2020

- Measures the average level of trust towards social institutions in a country

Trust is driven by both competence and ethical behaviour of institutions:

To drive trust, ethical behaviours of an organisation are **3 times more important** than its competence!

Why is ethics so important? (cont.)

Edelman Trust Barometer 2018

*- Consumers show concerns about **data-driven marketing**:*

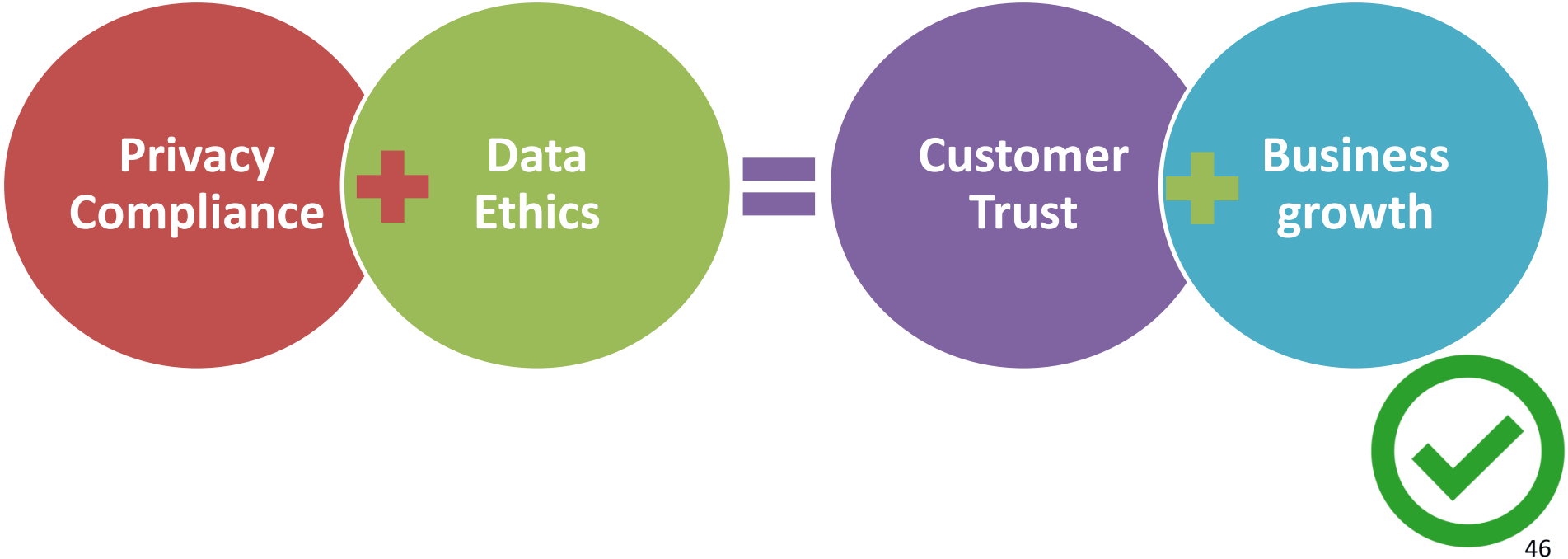
~50% respondents are **not willing to sacrifice some of their data privacy** in return for a more personalised shopping experience

50%+ and 60%+ respondents think **cross-site/cross-device tracking and psychological profiling** respectively are either **unfavourable or should be illegal**

70%+ respondents view **brands buying personal information** from another company the consumer does business with as **unfavourable or should be illegal**

High privacy expectation for brands:
83% respondents think **protection of privacy** and personal information is **one of the most important obligations** for business

With heightened privacy expectation of consumers…



Thank you

Stephen Kai-yi WONG, Barrister
Privacy Commissioner for Personal Data,
Hong Kong, China