

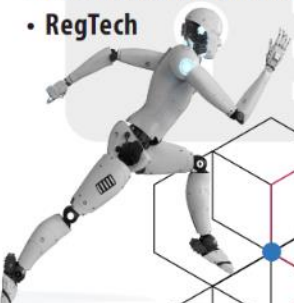


Webinar (Free of Charge)

*CPD POINTS: 3

“WORKING OUT FOR THE NEW DATA ECOSYSTEM AND LEGAL FRAMEWORKS”

- Privacy as a fundamental human right
- Data bombing
- Contraventions, Offences and Exemptions
- Handling data and data breaches
- Recent developments in major jurisdictions
 - EU, OECD, USA, New Zealand, Singapore, mainland of China
- Local data law amendments directions
- RegTech



SPEAKER

MR STEPHEN KAI-YI WONG

Barrister, Privacy Commissioner for Personal Data

ENROLLMENT:



**

DATE: 28 JULY 2020 (TUESDAY)

TIME: 2:30PM - 5:30PM

LANGUAGE: ENGLISH

www.pcpd.org.hk

https://www.pcpd.org.hk/spec_event/spec_event34_eng_apply.php

* This webinar has been recognised by professional bodies as a qualified training course.

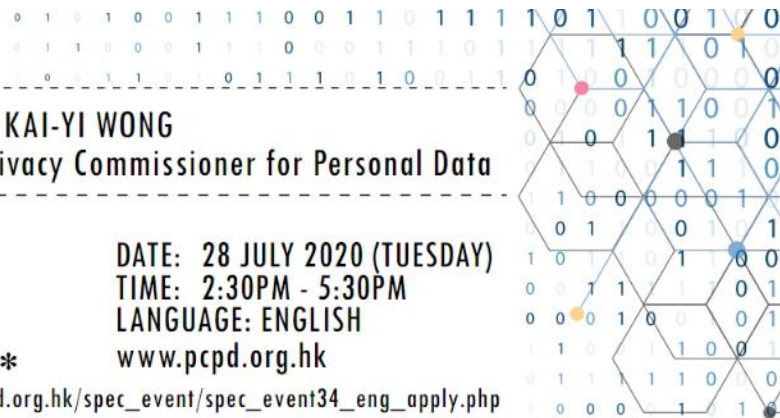
** This QR Code is provided by the PCPD. It takes you securely to the PCPD website where online registration can be done. You will only be asked to provide your name and email address. No other personal data of yours or others will be collected.

This webinar is for general publicity and education purposes only. During the webinar, no confidential or sensitive information will be transmitted. The PCPD recommends that the most up-to-date applications, anti-virus software and firewalls be installed. Security notes will be provided during online registration.

PCPD



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

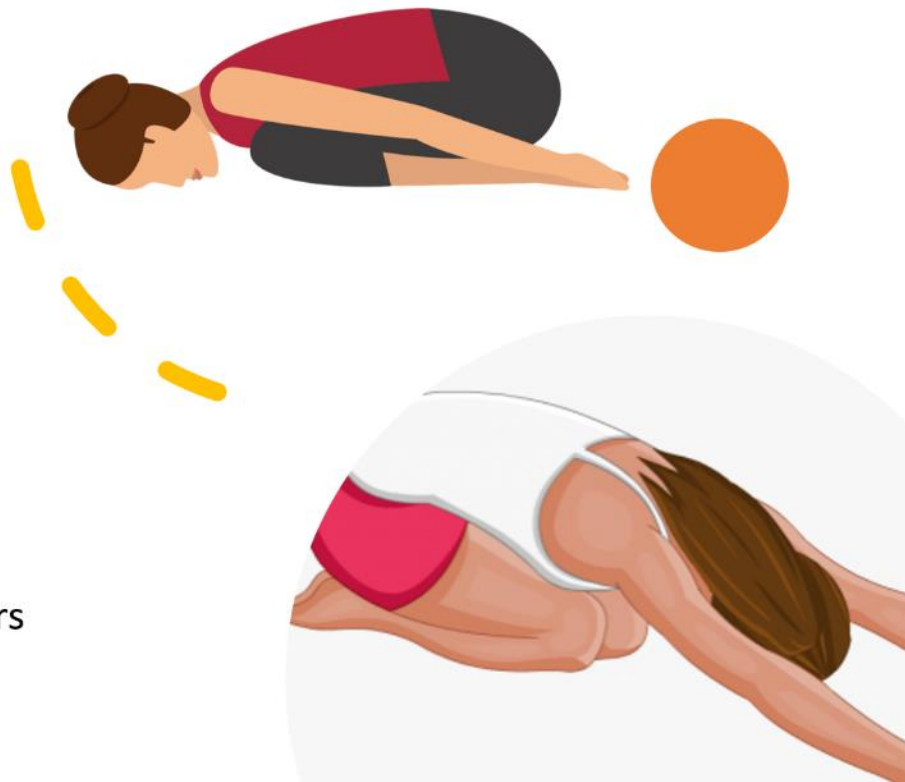


Warm Up

CHILD'S POSE (Balasana)

Benefits include:

- bringing total relaxation
- stretches the lower back and shoulders
- opens the hips
- helps fight insomnia

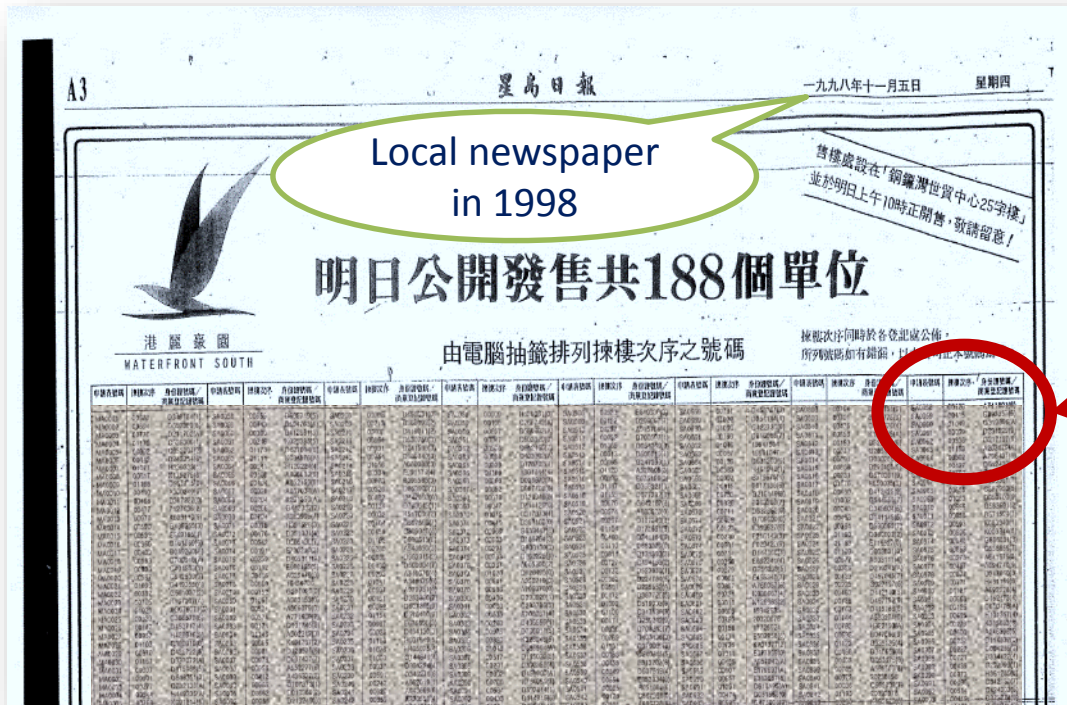


2

Data covers everyone of us from cradle to grave



Our sensitive personal data might even be publicly disclosed



Property Lottery Result

Announcement in 1998

申請表號碼	揀樓次序	身份證號碼 / 商業登記號碼
SA0808	00764	D 00051(5)
SA0809	00701	D 00051(1)
SA0810	00475	D 00051(1)
SA0811	00559	K 00051(1)
SA0812	00153	D 00051(0)
SA0813	00871	C 00051(3)
SA0814	00891	C 00051(7)

Full HKID Card number

Volume of data is growing exponentially

*“There were **5 Exabytes** of information created between the dawn of civilization through 2003, but that much information is now **created every 2 days.**”*

Eric Schmidt, Google, 2010
(Source: [World Economic Forum](#))

(Note: 1 Exabyte = 1 billion Gigabytes)

The proliferation of devices such as PCs and smartphones worldwide, increased Internet access ... has contributed to the **doubling of the digital universe within the past two years alone.**

IDC, 2012
(Source: [DELL Technologies - IDC Digital Universe study](#))

IDC predicted that the *“Global Datasphere”* would grow from **33 Zettabytes in 2018 to 175 Zettabytes by 2025.**

IDC, 2018
(Source: IDC White Paper *“[The Digitization of the World From Edge to Core](#)”*)

(Note: 1 Zettabyte = 1,000 Exabytes = 1 trillion Gigabytes)

5

Behind the huge value of e-commerce is huge volume of personal data

Sales on 'Double 11 Day'
on an e-commerce
platform in mainland



2017: RMB 168.2 billion sales



2018:
29% increase year-on-year



2019:
26% increase year-on-year

Value of data is increasing

*“Information is the **oil of the 21st century**, and analytics is the combustion engine.”*

Peter Sondergaard, Gartner Research, 2011
(Source: [Medium.com](https://medium.com))

*“The world’s **most valuable resource** is no longer oil, but data.”*

The Economist, 2017
(Source: [Economist.com](https://www.economist.com))

*“Data is the **most valuable asset of Alibaba**.*

The key objective of Tao Bao is not selling goods, but collecting retail and manufacturing data.

The key objective of Ant Financial is establishing a credit scoring system.

Our logistics operation is not aimed at delivering goods, but aggregating data.”

Jack Ma, Alibaba, 2014
(Source: [人民網 \(People.com.cn\)](http://www.people.com.cn) [Originally in Chinese])

7

Even beggars may collect your personal data through e-wallets



Source: [中國評論通訊社 \(CRNTT.com\)](http://www.crntt.com), 2017

Ubiquitous collection of data has created privacy and human right concerns

“The digital information ecosystem farms people for their attention, ideas and data in exchange for so called ‘free’ services.”

Giovanni Buttarelli, late European Data Protection Supervisor, 2018
(Source: [EDPS](#))

Emergence of AI deepens privacy and human right concerns

*“Artificial intelligence **challenges traditional notions** of consent, purpose and use limitation, transparency and accountability — the pillars upon which international data protection standards rest.”*

David Kaye, UN Special Rapporteur on the right to freedom of opinion and expression, 2018
(Source: [Report to UN General Assembly, August 2018](#))

*“... AI also opens the way for new types of **unfair differentiation** (some might say discrimination) that escape current laws.”*

Council of Europe, 2018

(Source: Council of Europe, [report on “Discrimination, artificial intelligence, and algorithmic decision-making”](#))

10

The world has started thinking about data ethics

*“Our own information, from the everyday to the deeply personal, is being **weaponized** against us with military efficiency.*

*... We don't do it because we have to. **We do it because we ought to.**”*

Tim Cook, Apple, 2018
(Source: 40th ICDPPC, Brussels)

*“Only if you think about **jobs, inclusiveness, security and privacy** will your company be sustainable and welcome in this century. Otherwise, you'd be out.”*

Jack Ma, Alibaba, 2019
(Source: [SCMP](#))

Data protection law is also responding to technological advancement

GDPR, Recital 6:

“Rapid technological developments and globalisation have brought new challenges for the protection of personal data.

“The scale of the collection and sharing of personal data has increased significantly.

“Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities.

“Technology ... should further facilitate the free flow of personal data ..., while ensuring a high level of the protection of personal data.”

12

Data protection is now an issue in international diplomacy and trade



“The harder issues [of the **China-US trade war**] are *‘industrial espionage, copyrights, ... privacy and security issues.’*”

Jim Costa, US Congressman, 2019
Source: [Reuters](#), 25 November 2019

“US ordered **closure of Chinese consulate in Houston** within 72 hours *‘in order to protect American intellectual property and Americans' private information.’*”

Source: [CNN](#), 22 July 2020

Privacy as a Fundamental Human Right

Benefits include:

- Improves balance and stability in the legs.
- On a metaphysical level, helps one to achieve balance in other aspects of life.
- Strengthens the ligaments and tendon of the feet.
- Strengthens and tones the entire standing leg, up to the buttocks.
- Assists the body in establishing pelvic stability.

TREE POSE
(Vrksasana)



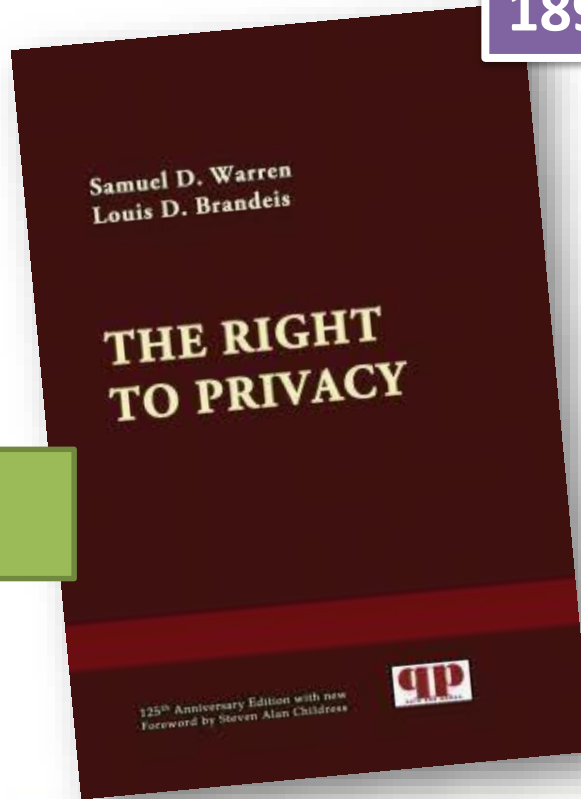
Right to be let alone



Samuel Warren

An attorney in Boston, USA

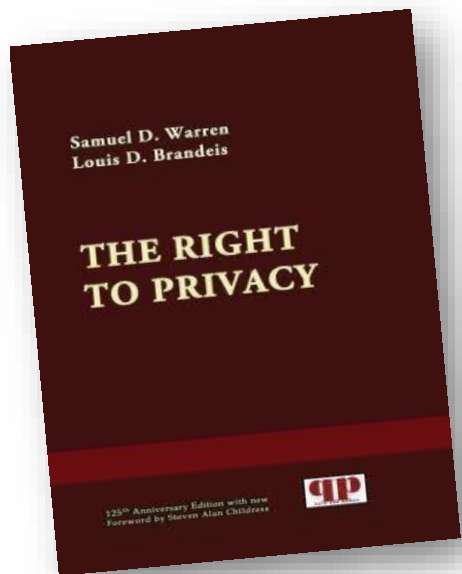
1890



Louis Brandeis

An American lawyer; served as a Justice at the US Supreme Court from 1916 to 1939

Significance of “*The Right to Privacy*” (1890)



- Right to privacy, as a legal concept, was **invented**
- Defined privacy as the “*right to be let alone*”
- Created momentum for modern discussions of privacy law



The Universal Declaration of Human Rights



Adopted by the United Nations General Assembly in Paris on 10 December 1948 as a common standard of achievement for all peoples and all nations

The first time that countries agreed on a comprehensive statement of inalienable human rights


Dr. Peng-chun Chang from mainland China was a member of the drafting committee

Recognised that *“the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world.”*

17

The Declaration is:

- not a treaty;
- not legally binding on countries; but
- widely considered as a part of customary international law.



*“All human beings are born free and equal in **dignity** and rights.”*

(Article 1)

*“No one shall be subjected to arbitrary interference with his **privacy**, family, home or correspondence.”*

(Article 12)

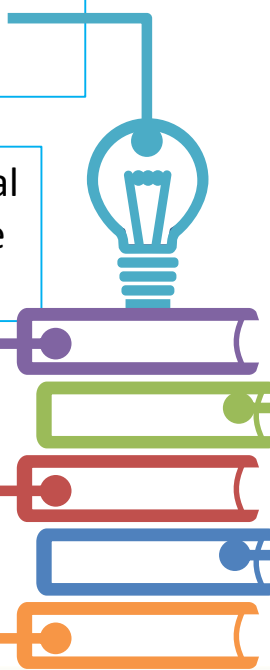
International Covenant on Civil and Political Rights (ICCPR)

Derived from the *Universal Declaration of Human Rights*

Adopted by the United Nations General Assembly in December 1966 and came into force in March 1976

Ratified by the UK in 1976, and **applied to Hong Kong** in the same year

People's Republic of China signed the ICCPR in 1998, but has not yet ratified it



Considered as the **International Bill of Human Rights** together with *Universal Declaration of Human Rights* and the *International Covenant on Economic Social and Cultural Rights*

Legally binding on the countries that ratify it

ICCPR Article 17 (1)

*“No one shall be subjected to **arbitrary or unlawful interference** with his **privacy**, family, home or correspondence.”*

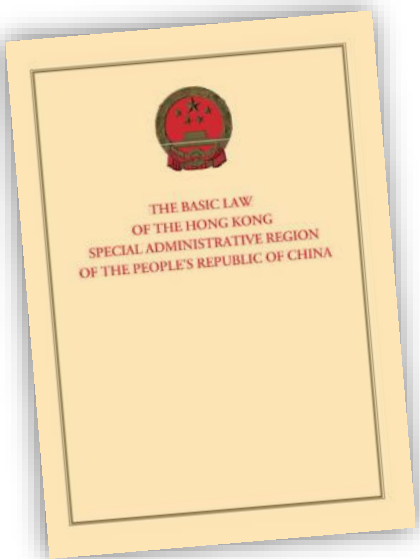
Hong Kong Bill of Rights Ordinance

Chapter 383 (BORO)

- Enacted and came into effect in June 1991
- Incorporated the ICCPR into the laws of Hong Kong
- Binds the Government and all public authorities
- **Article 14**, section 8, Part II of the BORO:
*“No one shall be subjected to **arbitrary or unlawful interference** with his **privacy**, family, home or correspondence, nor to unlawful attacks on his honour and reputation.”* [Cf. ICCPR Article 17(1)]

21

Basic Law of Hong Kong SAR

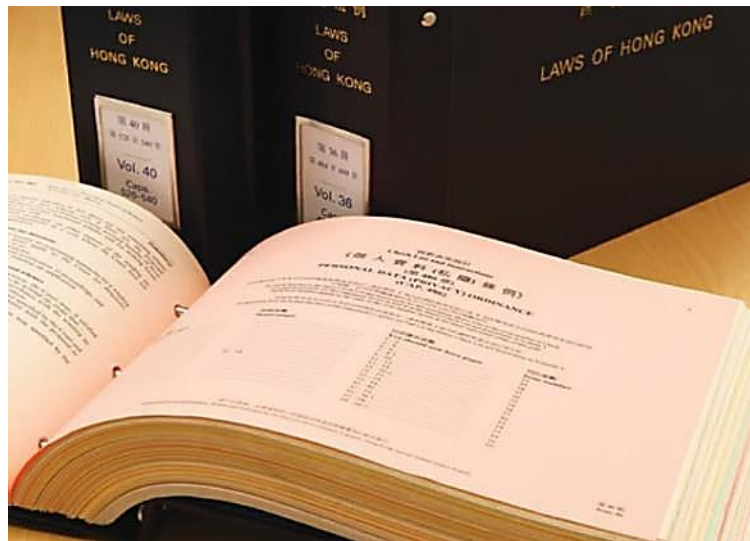


- Adopted on in 1990
- Came into effect on 1 July 1997
- **Article 30** provides constitutional guarantee that privacy right is a fundamental human right:
*“The freedom and **privacy of communication** of Hong Kong residents shall be protected by law.”*
- **Article 39** provides that the provisions of the **ICCPR** shall remain in force and shall be implemented through the laws of the Hong Kong

Personal Data (Privacy) Ordinance

Chapter 486 (PDPO)

- Enacted in 1995 and came into effect in December 1996
- With reference to OECD Privacy Guidelines 1980 and EU Directive 1995
- One of **Asia's longest standing** comprehensive data protection laws
- Origins in the August 1994 Law Reform Commission Report entitled "Reform of the Law Relating to the Protection of Personal Data"



23

Reasons for enacting the PDPO

(as per the 1994 Law Reform Commission Report)

Statutory protection of information privacy at that time was scattered and incidental in nature

Article 14 of the BORO provides some broad protection against public sector intrusion on privacy, but not against infringements by the private sector

ICCPR and BORO afford protection only to information upon a person's private life, not all information relating to an identifiable individual

Giving statutory force to internationally agreed data protection principles could:

- > discharge Hong Kong's obligation in human rights protection
- > retain Hong Kong's status as an international trading centre

24

Privacy right in Hong Kong SAR and the mainland

Hong Kong:

Privacy is firmly established as a **fundamental human right** by:

- application of **ICCPR** since 1976
- enactment of **BORO** in 1991 and the **PDPO** in 1995
- implementation of **Basic Law** in 1997

‘Human rights’ are “*the **inherent dignity** and ... the **equal and inalienable** rights of all members of the human family.*”
They are “*the foundation of freedom, justice and peace in the world.*”

[Source: Universal Declaration of Human Rights]

Mainland:

- Privacy right was **not recognised** in laws **until** the enactment of the Tort Law (《侵權責任法》) in December 2009
- Privacy right is a **civil right** (民事權益), on a par with property right, copyright and patent, pursuant to the Tort Law, Article 2
- Privacy right is recognised as a **personality right** (人格權) for the first time with the enactment of the Civil Code (《民法典》) in May 2020, on a par with the rights to life and health

‘Personality rights’ are the rights and interests enjoyed by a civil subject as derived from his personality **interest** (人格權是民事主體對其特定的人格利益享有的權利)

[Source: Introduction to the Civil Code by the NPC (全國人民代表大會常務委員會副委員長王晨, 關於《中華人民共和國民法典(草案)》的說明 (23 May 2020)]

WARRIOR POSE (Virabhadrasana)



Data Bombing



Benefits include:

- Help calm and steady your mind
- Strengthens shoulders, arms, legs, ankles and back
- Opens hips, chest and lungs
- Improves focus, balance and stability

26

Evolving Nature of Personal Data

- Privacy / personal data protection laws in most jurisdictions tend to focus on the protection of “personal data” – data that **identifies** an individual, or renders the person **identifiable**
- E.g. Personal Data (Privacy) Ordinance defines “personal data” as- any data:

*“... from which it is practicable for the **identity** of the individual to be directly or indirectly **ascertained**.”*

Personal Data - expanding

“Personal data” now incorporates a **constantly-expanding array of information** under many privacy / personal data protection laws, e.g.-

Location data

- GPS location
- Proximity to Wi-Fi or Bluetooth beacons
- Proximity to nearby mobile network towers

IP address

- Internet protocol address that identifies a computer
- May reveal approximate location of a user

Device identifier

- Unique information identifying a mobile device
- e.g. MAC address, IMEI number

Personal Data – expanding

Internet activity

- Browsing histories
- Search histories

Biometric information

- Facial, fingerprint, iris and retina images
- Gaits
- Genetic or DNA information

Consumer data

- Purchase histories
- Credit histories

Health & medical information

- Medical conditions
- Frequency of visiting doctors
- Contact-tracing information in times of COVID-19 pandemic

29

10100110100
10000101010
011110111011
011011010101
000011100101
0101000101



**Extent of
regulation by
privacy laws?**

30

Categories of Data

Examples of data in today's data-driven economy:

De-identified / aggregated data

- Identities of the individuals are no longer ascertainable
- Carries inherent risk of re-identification

Generated / derived / observed data

- Not provided by a data subject
- Generated during the use of electronic services
 - internet browsing activity
 - purchasing habits
 - location information

Focus on Protection – not data

The ecosystem of data is widening. There is an increasing **blurring of the boundaries** between data and personal data.

With increase in the use of connected devices, many types of data are likely to relate to “persons” one way or another.

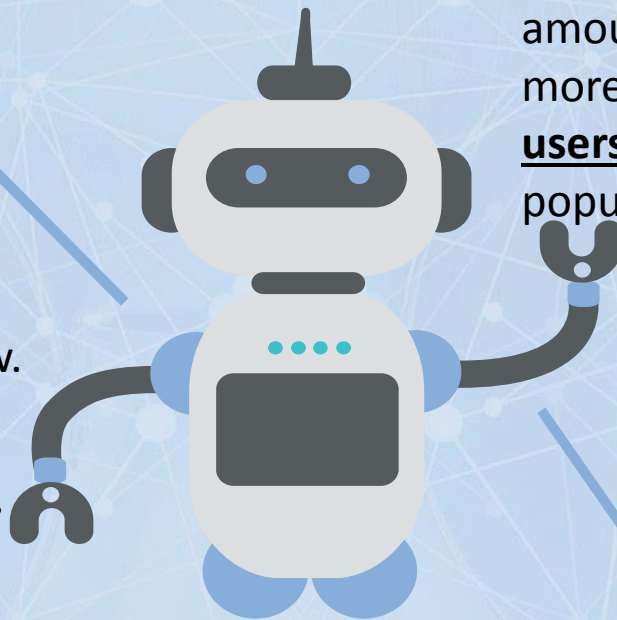
Instead of a theoretical analysis of whether data is “personal”, we **should focus on protecting individuals**, while facilitating the flow of data.

The Mainland of China's Advantage in AI

The mainland of China has laid out plans to become the global AI leader by 2030.

The National People's Congress Standing Committee has started reviewing a draft Data Security Law.

It aims to promote the use of data while protecting individual privacy.



The mainland of China's advantage in AI is the huge amount of data generated by its more than **900 million internet users**, the world's biggest online population.

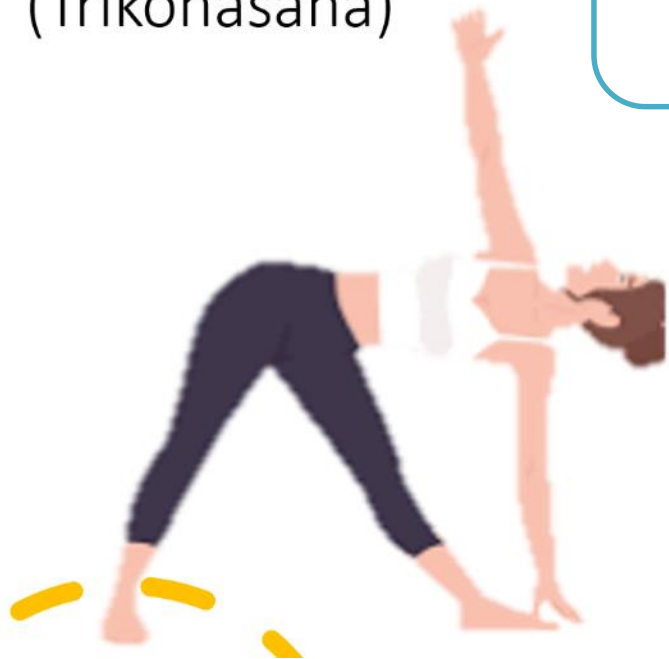
Value of Data and Trust

The immense value of data resides not only in the information that it provides, but also in its ability to train AI systems – to facilitate machine learning.

To achieve that, a massive volume of data is needed to provide an effective outcome: more data will likely provide better solutions.

For this reason, **maintaining trust in the ethical use and sharing of data is of paramount importance**. A loss of confidence will erode the quantity and quality of data available.

TRIANGLE POSE (Trikonasana)



Contraventions, Offences and Exemptions

Benefits include:

- Stretches legs, muscles around the knee, ankle joints, hips, groin muscles, hamstrings, calves, shoulders, chest and spine.
- Stimulates function of abdominal organs.
- Relieves stress.
- Improves digestion and constipation.



EU General Data
Protection Regulation
25 May 2018

GDPR

<https://www.marketersgo.com/market/201805/dg2-eu-gdpr-effect/>

35

Data breach incidents



<https://securityboulevard.com/2020/04/wappalyzer-reveals-data-breach-after-hacker-disclosed-incident-to-customers/>

36

UK ICO's intention to fine British Airways £183.39m under GDPR

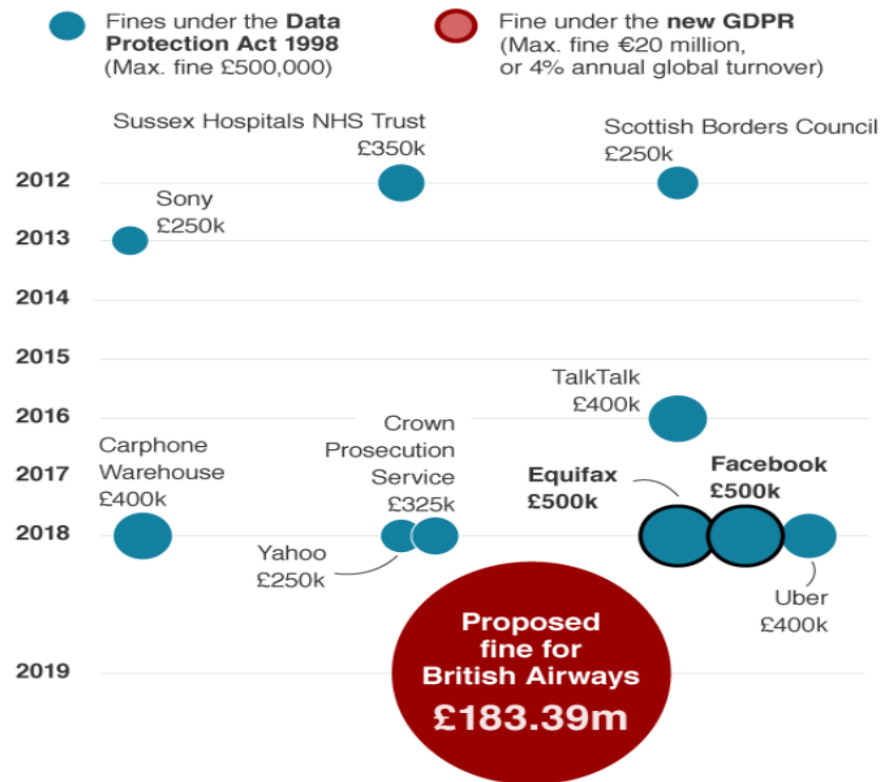


<https://www.reflectiz.com/british-airways-magecart-third-party-breach-leads-to-a-230-million-gdpr-fine/>

37

Biggest fines for data breaches

Fines over £250,000



<https://blazon.online/privacy/british-airways-faces-record-183m-fine-for-data-breach/>

Source: ICO - Information Commissioner's Office

BBC

UK ICO also fined CX £500,000, the maximum fine imposed under the UK Data Protection Act 1998



39

PCPD



H K



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

	British Airways	Cathay Pacific
Timing of Breach(es)	2018	2014 – 2018
Customers Affected	c. 500,000	c. 9.4 million
Details of Breach	Failure to secure JavaScript vulnerability leading to diversion of user traffic to a fake website	Multiple failures, including failure to update servers to combat known vulnerability, failure to implement two factor authentication and allowing administrator console to be accessed via the internet
Information Compromised	Personal details, credit card information, log in details, travel booking information	Personal details, passport numbers, travel booking information, historical travel information
Applicable Law	Data Protection Act 2018 (UK) (enacting the General Data Protection Regulation (EU) 2016/679)	Data Protection Act 1998 (UK)
Fine Levied by ICO	£183.4m (c. A\$367m)	£500,000 (c. A\$1m)

More security breach incidents ...

- (January 2019) **The French Data Protection Authority (CNIL) fined Google €50 million for GDPR violations**

(Source: <https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc>)

- (May 2020) **Irish Data Protection Commission fined a state agency €75 million for GDPR breach**

(Source: <https://www.dataprotection.ie/en/irish-dpc-submits-article-60-draft-decision-inquiry-twitter-international-companys-compliance>)

中信銀行洩客戶資料 銀保監會啟立案調查

香港文匯報訊 據中新社報道，中國銀保監會消費者權益保護局9日就中信銀行侵害消費者合法權益一事進行通報。通報稱，該局將按照相關法律法規，啟動立案調查程序，嚴格依法依規進行查處。

5月6日，內地脫口秀演員王越池（藝名「池子」）在微博上發文稱，中信銀行上海虹口支行在未經其授權、未經任何司法機關合法調查程序的情況下，將其個人銀行賬戶交易明細提供給與其發生經濟糾紛的笑果文化公司，侵犯了個人隱私。

涉嫌違反商業銀行法

該事件在互聯網上迅速引起關注。5月7日凌晨，中信銀行發表道歉信承認洩露客戶信息一事屬實，稱該行已按制度規定對相關員工予以處分，並對支行行長予以撤職。

銀保監會消保局通報指出，2020年3月，中信銀行在未經客戶本人授權的情況下，向第三方

提供個人銀行賬戶交易明細，違背為存款人保密的原則，涉嫌違反《中華人民共和國商業銀行法》和銀保監會關於個人信息保護的監管規定，嚴重侵害消費者信息安全權，損害了消費者合法權益。

通報表示，各銀行保險機構要引起警示，嚴格按照《中華人民共和國商業銀行法》《中華人民共和國保險法》和《中國銀保監會關於銀行保險機構加強消費者權益保護工作體制機制建設的指導意見》，認真執行相關法律法規和監管規定，依法合規開展經營活動，切實保護消費者合法權益。

根據《中華人民共和國商業銀行法》第二十九條規定，商業銀行辦理個人儲蓄存款業務，應當遵循存款自願、取款自由、存款有息、為存款人保密的原則。對個人儲蓄存款，商業銀行有權拒絕任何單位或者個人查詢、凍結、扣劃，但法律另有規定的除外。

8銀行違規被罰1970萬元

香港文匯報訊 據中新社報道，中國銀保監會官方網站9日一次性掛出9張罰單，涉及包括國有六大行在內的8家銀行，處罰金額達到1,970萬元（人民幣，下同）。

其中，中國農業銀行因監管標準化數據（EAST）系統數據質量及數據報送存在資金交易信息漏報嚴重、信貸資產轉讓業務漏報等違法違規行為，「兩會一層」境外機構管理履職不到位、信貸資金被挪用作保證金等原因分別收到兩張罰單，合計430萬元。

中國銀行上述系統數據質量及數據報送亦存在多項違法違規行為，包括理財產品數量漏報、資金交易信息漏報嚴重、貿易融資業務漏報等。根據《中華人民共

和國銀行業監督管理法》第四十六條和相關內控管理、審慎經營規定，銀保監會對其處以罰款合計160萬元。

此外，中國工商銀行、中國建設銀行、交通銀行、中國郵政儲蓄銀行等其他四家國有大行亦因不同原因被罰。同時收到罰單的銀行還有中信銀行、中國光大銀行兩家股份制銀行。上述罰單金額都達到百萬元級別。

近年來，中國金融監管力度不斷加大，市場亂象存量問題持續減少，增量問題得到有效遏制，一批重大非法集資案件得到嚴厲查處。銀保監會數據顯示，2019年，全系統共處罰銀行保險機構2,849家次，處罰責任人員3,496人次，罰沒合計14.49億元。

Offences under the PDPO

- Contravention of DPP is not an offence.
- A table summarising the various offences under PDPO and the respective penalties are available on the PCPD's website:

https://www.pcpd.org.hk/misc/files/table2_e.pdf

Offences under the PDPO

Selected offences to cover:-

- (1) Direct marketing offence;
- (2) Offences relating to the Commissioner's investigation powers; and
- (3) Criminal doxxing.

(i) Direct Marketing Offences

Revised Part 6A as a result of the 2012 amendment ordinance

- Direct marketing activities that are **not directed at “specified persons”** are **outside the scope** of the PDPO, e.g.-
 - 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”*
- See the Unsolicited Electronic Messages Ordinance (Cap 593), enforced by the Office of the Communications Authority

45

(i) Direct Marketing Offences

Regulate under the following 5 major aspects:-

- 1) the data user **must notify** the data subjects of certain prescribed information (sections 35C(2) and 35J(2));
- 2) the notification must be easily **understandable and readable** (sections 35C(4) and 35J(4));
- 3) the data user must provide a **response channel** for the data subjects to communicate his consent or indication of “no objection” to the intended use or provision of the data (sections 35C(2) and 35J(2));

46

(i) Direct Marketing Offences

- 4) the data user must obtain the relevant data subject's **consent** or indication of "**no objection**" before using the data subject's personal data in direct marketing (sections 35E(1) and 35K(1)); and
- 5) the data user must cease using the data subject's personal data in direct marketing without charge if the data subject so requires, i.e. **opts out** (sections 35F(1), 35G(1) and 35L(1)).

(i) Direct Marketing Offences

The Commissioner recommends ensuring **transparency** and **explainability** as the keys such that it would be a good practice for data users to observe the following principles (which are non-exhaustive):

- a) **Respect** data subject's right of self-determination of his own personal data;
- b) Be **accountable, open and transparent** in the handling of personal data including clearly identifying to the data subject the data user whom the direct marketer represents;

48

(i) Direct Marketing Offences

- c) Give individuals an **informed choice** of deciding whether or not to allow the use of their personal data in direct marketing;
- d) Present information regarding the collection, use or provision of personal data in a manner that is **easily understandable** and, if in written form, **easily readable** (e.g. providing information in large prints for the aged and those with impaired vision); and
- e) Honour and update the data subject's request for ceasing the use of his personal data in a professional and **timely** manner.

(i) Direct Marketing Offences

Consent Requirement

Article 7 and Recital 32 of GDPR are good references:-

Voluntary

Specific

Informed

Unambiguous

(ii) Commissioner's Investigation Powers

- Lack of power to conduct search and seizure
- Lack of criminal investigation and prosecution powers
- Section 43 of PDPO:
 - the Commissioner may, for the purposes of any investigation, be furnished with **any information, document or thing**, from such persons and make such inquiries, as he thinks fit.

51

(ii) Commissioner's Investigation Powers

- Section 44 of PDPO:
 - To **summon any witness** for examination, for furnishing any information or production of any document in that witness's possession or control which, in the Commissioner's opinion, may be relevant for the purpose of an investigation.
 - A witness who fails to appear before the Commissioner pursuant to the summons, or who intentionally evades personal service of the summons upon him will be **liable to prosecution** under section 50B

52

(iii) Criminal Doxxing (Weaponisation of Personal Data)

Section 64 of the PDPO (Offences for disclosing personal data obtained without consent from data users) provides:-

...

(2) *A person commits an offence if—*

*(a) the person discloses any personal data of a data subject which was obtained from a data user **without the data user's consent**; and*

*(b) the disclosure causes **psychological harm** to the data subject.*

(3) *A person who commits an offence under subsection (1) or (2) is liable on conviction to a **fine of \$1,000,000** and to **imprisonment for 5 years**.*

53

(iii) Criminal Doxing (Weaponisation of Personal Data)

- Around **5,000** doxing cases since June 2019

Actions taken by the PCPD:

- Approached and written to operators of platforms over 180 times
- Requested removal of over 3,000 links to doxing posts, 60% of which have been removed
- Investigated and referred over 1,400 cases to the Police

54

(iii) Criminal Doxxing (Weaponisation of Personal Data)

The Commissioner's difficulties ...

- Lack of **criminal investigation powers** – suspected cases of contraventions have to be referred to the Police
- Lack of **prosecution power** – whether prosecutions should be preferred is for the DoJ to evaluate, by taking into account all circumstances of the case, including whether any other criminal offences provided by other ordinances would be more appropriate.

55

(iii) Criminal Doxxing (Weaponisation of Personal Data)

Relevant Court case:-

- **DCCC 164/2020**
 - The first case to be charged under section 64(2) (i.e. criminal doxxing)
 - Other charge – section 161 of the Crimes Ordinance (i.e. access to computer with criminal or dishonest intent)
 - Substantive hearing scheduled on 7 September 2020

56

(iii) Criminal Doxxing (Weaponisation of Personal Data)

2 Injunction cases:-

- **[2019] HKCFI 2773 (HCA 1957 of 2019)**
 - *Secretary for Justice & Commissioner of Police v Persons unlawfully and wilfully conducting themselves in any of the acts prohibited under paragraph 1(A), (B) or (C) in the indorsement of claim*
- **[2019] HKCFI 2809 (HCA 2007 of 2019)**
 - *Secretary for Justice v Persons unlawfully and wilfully conducting themselves in any of the acts prohibited under paragraph 1(a) and (b) in the indorsement of claim and the Internet Society of Hong Kong Limited*

57

- **The 1st case:- [2019] HKCFI 2773 (HCA 1957 of 2019)**
 - Hon Chow J of High Court **granted an injunction** order on 25 October 2019. (amended on 28 Oct, 1 Nov, 8 Nov and 10 Dec 2019).
 - On 8 November 2019, Hon Coleman J allowed the application made by the Hong Kong Journalists Association seeking an **exemption** of the injunction based on “**news activity**” (in accordance with the definition under section 61 of the PDPO).
 - Hon Coleman J allowed the **addition of “news activity” exemption**.
 - Lawful and proper reporting and freedom of the press, acting as a “watchdog”, were important in Hong Kong.
 - The adding of the exemption might also be beneficial in identifying the difference between real journalists performing lawful journalistic activity and fake journalists whose activity would not be expected to be included within the statutory definition of “news activity”.

58

Hysan Development Company Limited v Town Planning Board – Proportionality Test



- Is there a **pressing need** for such measures?
- Would these measures pursue a **legitimate aim**?
- Is there a **rational connection** between these measures and the legitimate purposes?
- Are these measures **no more than necessary** to achieve the legitimate purposes?
- whether a **reasonable balance** has been struck between the societal benefits of the encroachment and the inroads made into the constitutionally protected rights of the individual?

(i.e. not imposing an unacceptable harsh burden on the affected individuals?)

59

(iii) Criminal Doxxing (Weaponisation of Personal Data)

Relevant Court case:-

- **HCMP 249/2020**
 - Contempt of Court – contravention of court injunction against doxxing of police officers in [2019] HKCFI 2773
 - Sentenced on 17 June 2020
28 days of imprisonment, suspended for a year

Difficulties encountered when handling doxxing cases



No criminal investigation and prosecution powers



Difficult to trace the identities of doxxers



Difficult to prove the doxxing materials are obtained from a data user without the data user's consent



Most of the doxxing posts are hosted by overseas social media platforms

Doxxing regulation in other jurisdictions

Major jurisdictions usually do not have specific provision for doxxing in data protection laws

Network Enforcement Act of Germany provides administrative measures to compel social media platforms to remove improper online materials

Harmful Digital Communications Act of New Zealand allows victims of cyberbullying to apply for court order against social media platforms to take down unlawful materials

Singapore amended the *Protection from Harassment Act* in 2019 to prohibit disclosure of identity information with an intent to cause alarm or distress to the target persons or related persons (i.e. doxxing)

Possible ways of tackling doxxing

- Introduce legislative amendments to specifically address doxxing
- Confer on the Commissioner statutory powers to:
 - ✓ Request the **removal of doxxing contents** from platforms/websites
 - ✓ Carry out **criminal investigation and prosecution**

International Collaboration

- 41st International Conference of Data Protection and Privacy Commissioners (now renamed the Global Privacy Assembly) in Tirana, Albania in 2019
- In light of the borderless flow and transfer of personal data, the Commissioner joined other members to **co-sponsor a resolution on combating violence, hatred and extremist content on social media and on internet**. The resolution was passed by the conference.
- Doxing activities of this kind not only amount to a criminal offence under the PDPO, they also violate data ethics adopted in many other places. It is a total disregard for personal and public interest. It is definitely illegal and is totally unacceptable in our society.

64

Exemptions under the PDPO

Part 8 of the PDPO (sections 51A to 63D)

- Section 57 – **Security**
- Section 58 – **Crimes**
- Section 59 – **Public Health**
- Section 60B – **Legal Proceedings**

Exemptions under the PDPO

- ***Cinepoly Records Co. Ltd. and Others v Hong Kong Broadband Network Ltd and Others [2006] 1 HKLRD 255***

*"36. The Ordinance creates for the first time in Hong Kong statutory protections of privacy of individuals in relation to personal data. But the protections cannot be absolute. For there are obviously cases where **public interest** or **competing private rights and interests** may require such protections to be removed. Thus the Ordinance also creates certain exemptions : see Part 8. The exemptions can basically categorized into (a) public interest exemptions and (b) competing private interests exemptions.*

66

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.”

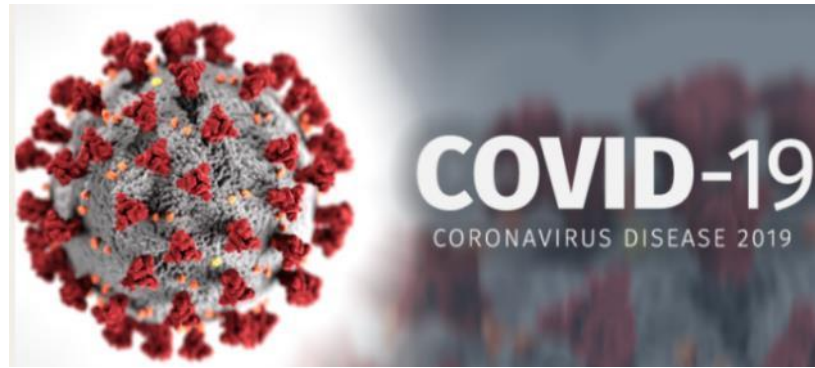
Hong Kong Bill of Right Ordinance (BORO)

- 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**

67



- Right to life is a supreme right and a pre-requisite for the enjoyment of all other human rights
(Source: Human Rights Committee of the United Nations, November 2018)
- Privacy right is not absolute but subject to restrictions
(see Article 4(1) of the ICCPR and section 5 of the BORO)

<https://fscluster.org/coronavirus>

Exemption: News Activity

- Section 61 strives to strike a fair balance between upholding the freedom of the press essential to journalists and the protection of the personal data privacy rights of individuals.
- Protection afforded under two limbs:-
 - data users engaging in news activity (determined from its nature of activities involved, hence not necessarily limit to traditional media organisations but also online media); and
 - informants in providing source of information to media organisations.

Exemption: News Activity

- Section **64(4)(d)** of the PDPO provides an exemption such that the person who disclosed the personal data for the purpose of a news activity and had reasonable grounds to believe that the publishing or broadcasting of the personal data was in the public interest.

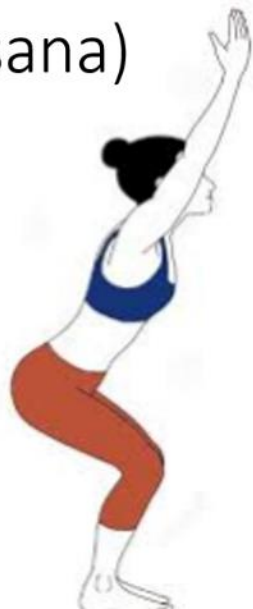
<https://news.un.org/en/story/2018/03/1005751>



70

Handling Data and Data Breaches

CHAIR POSE (Utkatasana)



Benefits include:

- Strengthen your thighs, which helps to stabilize your knees.
- Strengthen your lower back and glutes.
- Fire up your core muscles, which leads to improved abdominal strength.

What is a data breach?

- **Data Protection Principle 4:** Data users shall take all practicable steps to prevent unauthorised or accidental access, processing, erasure, loss or use of personal data.
- **Definition of “personal data breach”:** A data breach is a suspected breach of security exposing personal data to the risk of unauthorised or accidental access, processing, erasure, loss or use.

How to handle a data breach?



Immediate gathering of essential information relating to the breach



Contacting the interested parties and adopting measures to contain the breach



Assessing the risk of harm



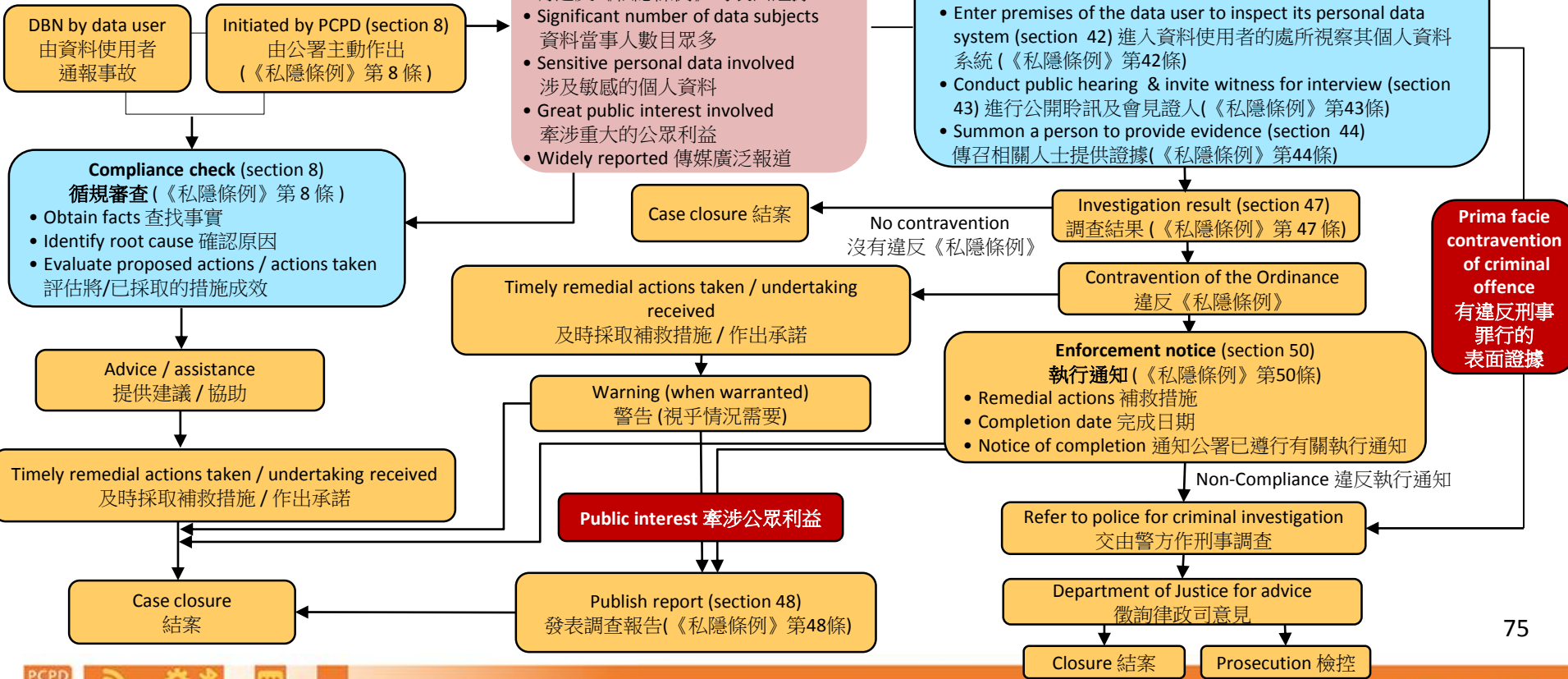
Considering the giving of data breach notification

73

How to report a data breach?

- Report to the data subjects affected
- Report to the Commissioner by means of the “Data Breach Notification Form”
- Submit the completed form to us online, by fax, in person or by post
- Details: https://www.pcpd.org.hk/english/enforcement/data_breach_notification/dbn.html

Handling a Data Breach 處理資料外洩事故



Recent Development in Major Jurisdictions

Benefits include:

- Stimulates Blood Circulation
- Stimulates abdominal organs, ovaries and prostate gland, bladder, and kidneys.
- Stimulates the heart **and improves general circulation.**
- Stretches the inner thighs, groins, and knees.
- Helps relieve mild depression, anxiety, and fatigue.
- Soothes menstrual discomfort and sciatica.

BUTTERFLY POSE
(Baddha Konasana)

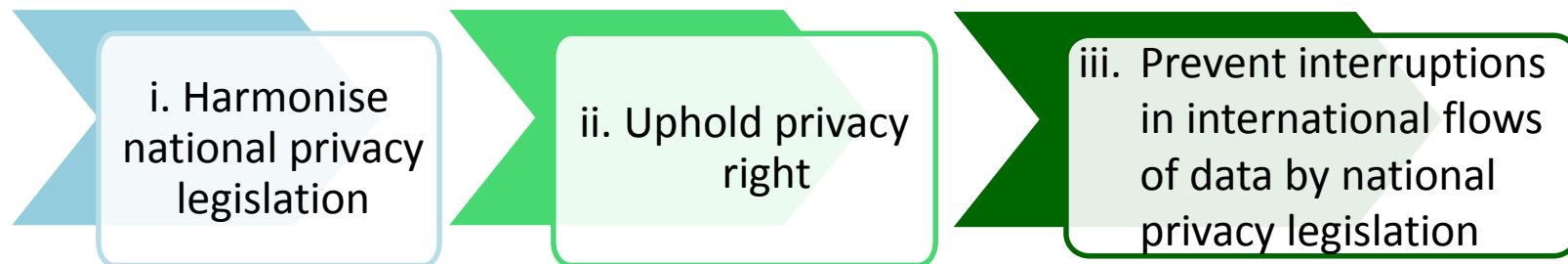


The OECD Guidelines 1980

Organisation for Economic Co-operation and Development

- The first internationally-agreed privacy principles

Objectives:

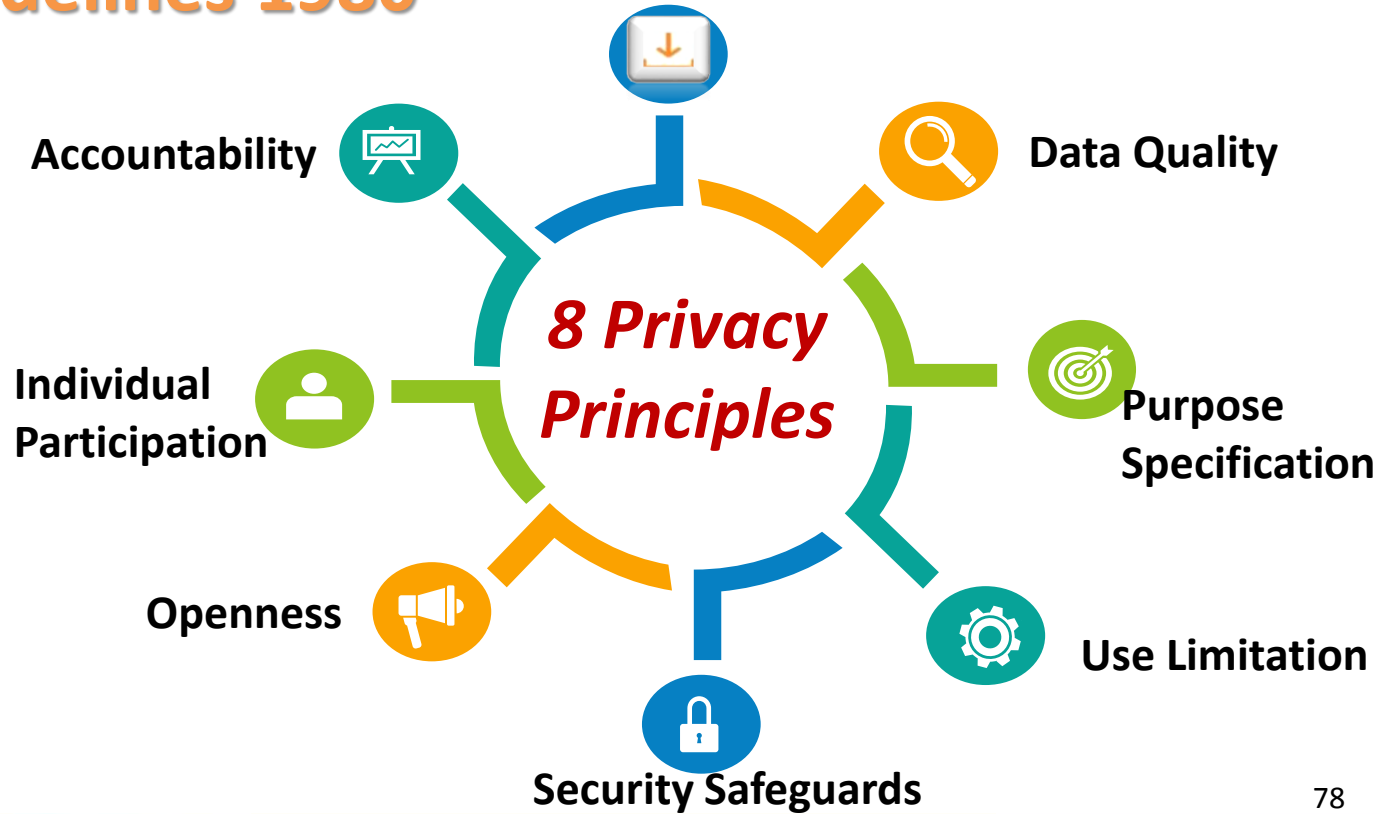


- Updated in 2013, the Guidelines remain an essential benchmark for the rules and practices in protecting personal data

The OECD Guidelines 1980

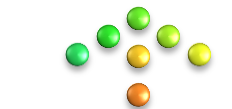


Collection Limitation



The OECD Revised Guidelines (2013)

**New concepts
introduced**



**Implementation of Privacy
Management Programme**



Data breach notification

Review of the implementation of the OECD Privacy Guidelines 2013

Questionnaire



Consulted 29 countries



Roundtable discussions

Focused research papers



80

Preliminary Findings of the Review

- The OECD Privacy Guidelines remain a **useful policy standard and benchmark** on which countries could base their own national legislation
- Further implementation guidance and analytical work considered helpful on topics such as:
 - the impact of emerging technologies
 - data subjects' rights (particularly data portability)
 - accountability
 - data ethics
 - privacy enhancing technologies

The EU GDPR- Data Protection as a Fundamental Human Right

Main features

One set of rules for all companies operating in the EU

People have more control over their personal data

Businesses benefit from a level playing field

The EU GDPR – 2 Years on

- **Surge of Complaint cases**

- EU & EEA in total (25 May 2018 - 30 Nov 2019): **275,000+**
- UK ICO (2018-19) :**41,661** (double 2017-18)
- Irish DPC : **7,215** (75% increase on 2018)

- **Mandatory Data Breach Notifications**

- EU & EEA in total (25 May 2018 – 27 Jan 2020): **160,000+**



Sanctions: Administrative Fine

- **Up to €20 million or 4% of the total worldwide annual turnover, whichever is higher**
- Common contraventions:
 - Principles relating to processing of personal data
 - Lawfulness of processing
 - Conditions for consent
 - Processing of sensitive personal data
 - Transparency and rights of data subjects
 - Security of processing and data breaches

Notable Sanctions

- French authority CNIL vs Google
- €50 million
- Lack of transparency and valid consent in conducting advertisement personalisation

- Decision affirmed by the French top court (June 2020)
- Google had not provided clear enough information for consent to be lawfully obtained — including objecting to a pre-ticked checkbox.
- Given Google's financial position, €50 million is not disproportionate.



Notable Sanctions

- Italian authority vs Telecom Company
- €27.8 million
- Making marketing calls without valid consent and lack of accountability (February 2020)

- Complainants claimed that they had received unwanted marketing calls, without having provided their consent or despite having registered on an opt-out list.
- Impacted several million individuals
- The fine: 0.2% of the company's total annual turnover



Important Guidelines Issued

Extra-territorial Application

- Apply if an organisation:
 - has an **establishment in EU** + personal data processed in the context of the activities of the establishment regardless of whether data processing in EU
 - does not have an establishment in EU but **offer goods or services** to or **monitor** the behaviour of individuals in EU
- *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)*

Important Guidelines Issued

Enhanced Right to Erasure/ Right to be Forgotten

- Right to require deletion of personal data without undue delay if:
 - Personal data is **no longer necessary** for the collection purpose
 - Individual **withdraws the consent** (which forms the basis of processing)
 - No overriding legitimate interest** on the part of the data controller
 - Personal data collected is about **children** in relation to an information society service
- Subject to exceptions, e.g. freedom of expression and information, public interest
- *Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engines cases under the GDPR (part 1)*

The EU GDPR & Free Flow of Data

Recital 101

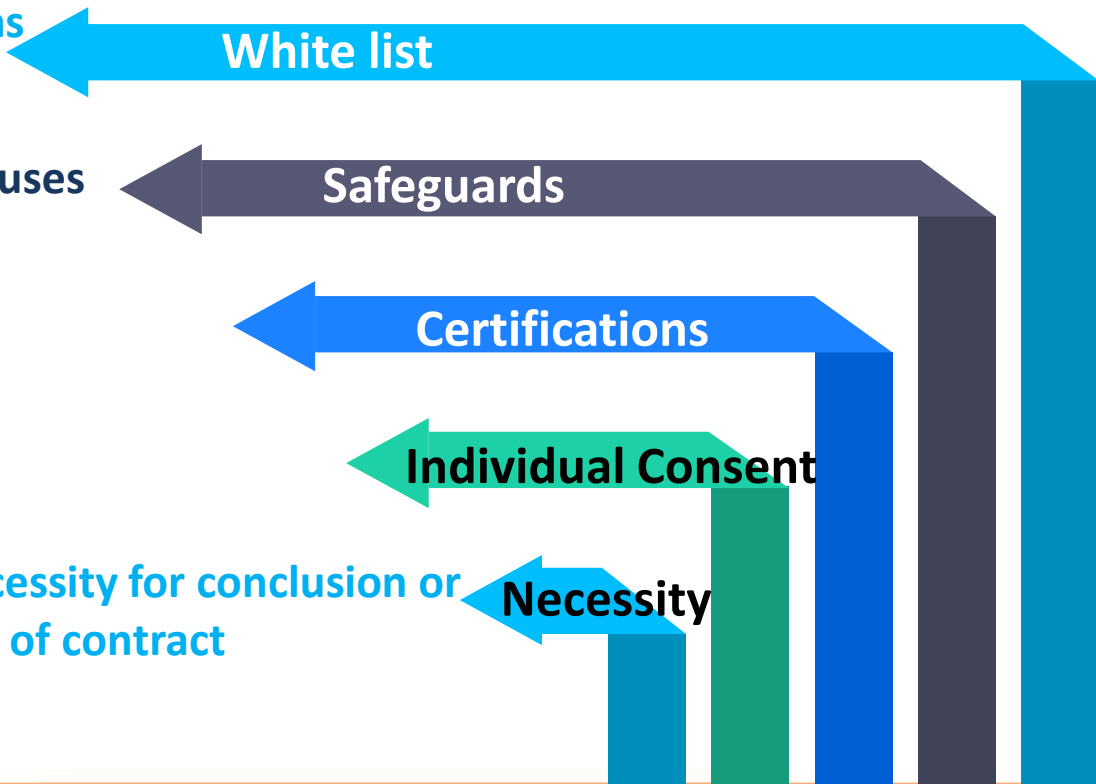
Flows of personal data across EU border are **necessary** for the **expansion of international trade and cooperation**

Personal data transferred from the EU to a place outside the EU will be afforded with **comparable protection**

Allowable cross-border data transfer under the GDPR

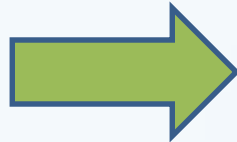
Examples

- EU's adequacy decisions
- EU-US Privacy Shield
- Standard contractual clauses
- Binding corporate rules



Sanctions

FAILURE to comply with the lawful requirements for transferring personal data to a recipient in a third country or international organisation



the **HIGHER** tier of administrative fines
i.e. up to €20 million or 4% of the total worldwide annual turnover, whichever is higher

Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Schrems II)

- The European Court of Justice has invalidated the EU-US Privacy Shield but has allowed standard contractual clauses to remain in place.

16 July
2020

The CJEU said **US surveillance and national security laws** invalidate the Privacy Shield decision. The limitations on the protection of personal data arising from the domestic law of the United States ... are **not circumscribed** in a way that satisfies requirements that are essentially equivalent to those required under EU law.



The CJEU also ruled that the Privacy Shield framework does **not give EU individuals actionable rights** before a body offering guarantees that are substantially equivalent to those required under EU law. The Ombudsperson mechanism is **insufficient**.

Impact of the Decision

- All transfers of personal data from the EU and the European Economic Area to the US under the EU-US Privacy Shield must be **reassessed**.
- All such transfers on the basis of the EU-US Privacy Shield must be **replaced by another legal basis** for transfer, such as :
 - the Standard Contractual Clauses (between organisations), Binding Corporate Rules (among the affiliates of one organisation), or individual consent.
- The legal regime in the destination countries, even under SCCs, must be taken into account to ensure that local laws do not prevent compliance with the SCCs.

Regulator's Responses



EDPS Wojciech Wiewiórowski: *“European supervisory authorities have the duty to **diligently enforce the applicable data protection legislation** and, where appropriate, to **suspend or prohibit transfers of data to a third country**. As the supervisory authority of the EU institutions, bodies, offices and agencies, the EDPS is carefully **analysing the consequences** of the judgment on the contracts concluded by EU institutions, bodies, offices and agencies.”*

EDPS (17 July 2020)

Source : https://edps.europa.eu/press-publications/press-news/press-releases/2020/edps-statement-following-court-justice-ruling-case_en

95

Regulator's Responses

“The EDPB **welcomes** the CJEU’s judgment, which highlights the fundamental right to privacy in the context of the transfer of personal data to third countries.

“... the **EU and the U.S. should achieve a complete and effective framework** guaranteeing that the level of protection granted to personal data in the U.S. is essentially equivalent to that guaranteed within the EU, in line with the judgment.”
(EDPB, 17 July 2020; Source 1)

Frequently Asked Questions on the judgment were issued on 23 July 2020.

(EDPB, 23 July 2020; Source 2)

Source 1: https://edps.europa.eu/press-publications/press-news/press-releases/2020/edps-statement-following-court-justice-ruling-case_en

Source 2: https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118.pdf

Regulator's Responses



An Coimisiún um
Chosaint Sonraí
Data Protection
Commission

Irish Data Protection Commission **strongly welcomes** the CJEU judgment. The judgment firmly endorsed the substance of the concerns expressed by the DPC and by the Irish High Court to the effect that EU citizens do not enjoy the level of protection demanded by EU law when their data is transferred to the United States. The Court also agreed with the DPC's view that, whatever mechanism is used to transfer data to a third country, the protection afforded to EU citizens in respect of that data must be essentially equivalent to that which it enjoys within the EU.

Irish Data Protection Commission (16 July 2020)

Source: <https://www.dataprotection.ie/en/news-media/press-releases/dpc-statement-cjeu-decision>

97



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

New Laws/Bills

<u>Jurisdiction</u>	<u>Status</u>	<u>Law (Amendments shown in bracket [non-exhaustive])</u>
Australia	Amendment Implemented in Feb 2018	The Privacy Act 1988 <i>(Mandatory Data Breach Notification)</i>
Brazil	New Passed in Aug 2018 (expected implementation in August 2020)	General Data Protection Law (LGPD)
California, US	New Implemented in Jan 2020	California Consumer Privacy Act (CCPA)
Canada	Amendment Implemented in Nov 2018	Personal Information Protection and Electronic Documents Act (PIPEDA) <i>(Mandatory Data Breach Notification)</i>
India	New Proposed in Dec 2019	Personal Data Protection Bill, 2019
Japan	Amendment Passed in Jun 2020 (expected effective in Q4 2021 or Q1 2022)	Amendments to the Act on the Personal Information Protection Law (APPI) <i>(Mandatory Data Breach Notification)</i>

98

New Laws/Bills(cont.)

<u>Jurisdiction</u>	<u>Status</u>	<u>Law (Amendments shown in bracket [non-exhaustive])</u>
New Zealand	Amendment Passed in Jun 2020 (will be implemented in Dec 2020)	New Privacy Bill to replace The Privacy Act 1993 <i>(Mandatory Data Breach Notification)</i> <i>(Extra-territorial application)</i>
Singapore	Amendment Proposed in May 2020	Personal Data Protection Act 2012 (PDPA) <i>(Mandatory Data Breach Notification)</i> <i>(Accountability)</i> <i>(New legal basis for data processing - legitimate interest)</i> <i>(Data portability)</i>
South Korea	Amendment Passed in Jan 2020	Amendments to the Personal Information Protection Act (PIPA) <i>(Permit the use of pseudonymised data without obtaining data subjects' consent)</i> <i>(Permit the use of personal data to an extent reasonably related to the original purpose)</i>
Thailand	New Passed in May 2019 (most provisions effective from May 2021)	Personal Data Protection Act (PDPA)

99

Common requirements in new data protection laws/bills

Jurisdiction	Accountability requirements	Mandatory Data Breach Notification	Right To Be Forgotten	Administrative Fines	Extra-territorial Application
EU	✓	✓	✓	✓	✓
Australia	✓	✓	X	X	✓
Brazil (not yet implemented)	✓	✓	X	✓	✓
California, US	X	✓	✓	X	✓
Canada	✓	✓	X	X	X
India (proposed)	✓	✓	✓	✓	✓
Japan	X	✓ (not yet implemented)	X	X	✓
New Zealand	X	✓ (not yet implemented)	X	X	✓ (not yet implemented)
Singapore	✓	✓ (proposed)	X	✓	✓
South Korea	✓	✓	✓	✓	X
Thailand (not yet implemented)	X	✓	✓	✓	✓

(considered "yes" by regulators, tough no explicit provision in the laws)



United States (US)

No comprehensive data protection law at Federal level

No general restrictions on data transfer at the federal level

Certain states have enacted laws (enforced by the **Attorney General**) limiting state agencies or state contractors from outsourcing data processing beyond US borders

Individuals' data privacy regulated by the **Federal Trade Commission** at the Federal level

101

California Consumer Privacy Act (CCPA)

- Took effect from **1 Jan 2020**
- Enforcement since **1 July 2020**
- Enforced by the Attorney General
- **✓** Extra-territorial effect
- Does not contain provision restricting cross-border data flow of data

CCPA – Scope

A business is subject to the CCPA if it

- i. is a **for-profit business** that collects and controls California residents' personal information
- ii. does business in the State of California, and
- iii. satisfies one of the following:
 - (a) annual gross revenues > US\$25 million; or
 - (b) receives or discloses the personal information of 50,000 or more California residents, households, or devices on an annual basis; or
 - (c) derives 50% or more of their annual revenues from selling California residents' personal information.

CCPA – Data Subjects' Rights

- Request **disclosure of how data is collected**, used and shared with third-party
- Require for **full erasure** of their data
- Request disclosure of whether data has been **sold** to third-party, to whom it was sold and ability to object to the sale of data
- **Opt-out** of the sale of their personal information

Enforcement of CCPA (1 July 2020)

- Civil enforcement actions taken by the Attorney General
- Violating businesses will be given a notice of non-compliance and a **30-day opportunity** to cure the non-compliance.
- Businesses who fail to comply within the 30-days will be subject to an injunction and a civil penalty:
 - > US\$2,500 for each unintentional violation, and
 - > US\$7,500 for each intentional violation.
- Customers can bring an action for statutory damages, if the consumer's non-encrypted and non-redacted personal information is subject to a qualifying data breach.

105

Children's Online Privacy Protection Act (COPPA)

Operators of commercial websites **directed at children** must provide **notice** and obtain **verifiable parental consent** before collecting personal information children under age **13**

Major requirements under the COPPA



PRIVACY POLICY NOTICE: must post prominent links on their websites to a notice of how they collect, use, and/or disclose personal information from children



PARENTAL NOTICE & CONSENT: must **notify parents** that they wish to collect information from their children and **obtain parental consent in advance**



LIMITED COLLECTION: must not collect personal information that is **more than reasonably necessary** to participate in the activity

107

Major requirements under the COPPA



RIGHT TO DELETION: must **allow parents** the opportunity to **review** and/or have their children's information **deleted**



DATA SECURITY: must **establish procedures** to protect the **confidentiality, security, and integrity** of children's personal information

Enforcement of the COPPA



Penalties imposed (up to USD\$42,530 per violation)



Required deletion of personal information collected without parental consent



Mandatory staff training



Written compliance report to FTC

New Zealand Privacy Act 2020

- Passed on 26 June 2020
- Took effect from 1 December 2020

Key Changes

(1) Mandatory privacy breach notification threshold: 'serious harm'.



Key Changes

(2) Extraterritorial effect

‘Carrying on business’ in New Zealand will be subject to the Act’s privacy obligations, even if it does not have a physical presence in NZ.

(3) Introducing new criminal offences

E.g. misleading an agency (i.e. data user) to access someone else’s personal information



(4) Regulate cross-border transfer/ disclosure of personal data

- the receiving party shall be subject to similar safeguards to those in the Privacy Act.

(5) Power to issue compliance notices and to direct agencies to provide individuals access to their personal information



Review of Singapore's Personal Data Protection Act (PDPA)

- Draft Bill was released for public consultation on 14 May 2020.
- If passed, the Bill will be the first amendment to the PDPA since it was passed in 2012.

5 Key amendments to the PDPA

(1) Mandatory Data Breach Notification

Organisations must notify:

- the **data protection authority** as soon as practicable (**No later than 3 days**)
- affected individuals as soon as practicable

5 Key amendments to the PDPA

(2) Increased Financial Penalty Cap:

- up to **10%** of an organisation's **annual gross turnover** in Singapore; or
- **S\$1 million**, whichever is higher

(3) Introduction of the Accountability Principle

Required organisation to demonstrate compliance (i.e. proper handling; safekeeping of personal data)

5 Key amendments to the PDPA

(4) Wider Scope for Deemed Consent

Cover circumstances where:

- i. the collection, use or disclosure of personal data is reasonably necessary to conclude or perform a contract or transaction; or
- ii. individuals have been notified of the purpose of the intended collection, use or disclosure of personal data, given a reasonable opportunity to opt-out, and have not opted out.

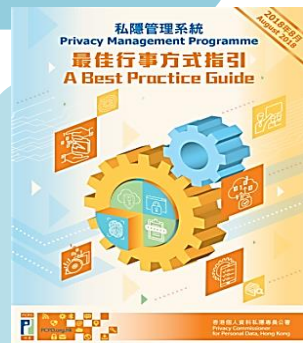
116

5 Key amendments to the PDPA

(5) Introduction of Data Portability Right

Individuals can request a copy of their personal data be transmitted to another data user, enabling consumers to switch service providers more easily.

Take a break. Download Our Publications.



Ethical Accountability Framework for Hong Kong, China

A Report prepared for the Office of the Privacy
Commissioner for Personal Data

Analysis and Model Assessment Framework



Recent developments of the privacy landscape in the mainland of China



119

PCPD



H K



PCPD.org.hk

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

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

Please scan here
to download



Cybersecurity Law

- ❖ Issued in November 2016
- ❖ Effective from 1 June 2017
- ❖ Implementing rules issued or drafted for consultation

Snapshot of China Cybersecurity Law

What is the CSL

- Data privacy and cybersecurity in China

Who are regulated

- Network operators - i.e. network owners, network administrators and network service providers
- NOT just telecom/internet companies
- NOT just Chinese domestic companies

Who are the regulators

- The Cyberspace Administration of China (國家互聯網信息辦公室)
- Ministry of Industry and Information Technology (工業和信息化部)
- Ministry of Public Security (公安部), etc.

Overview of Cybersecurity Law of China

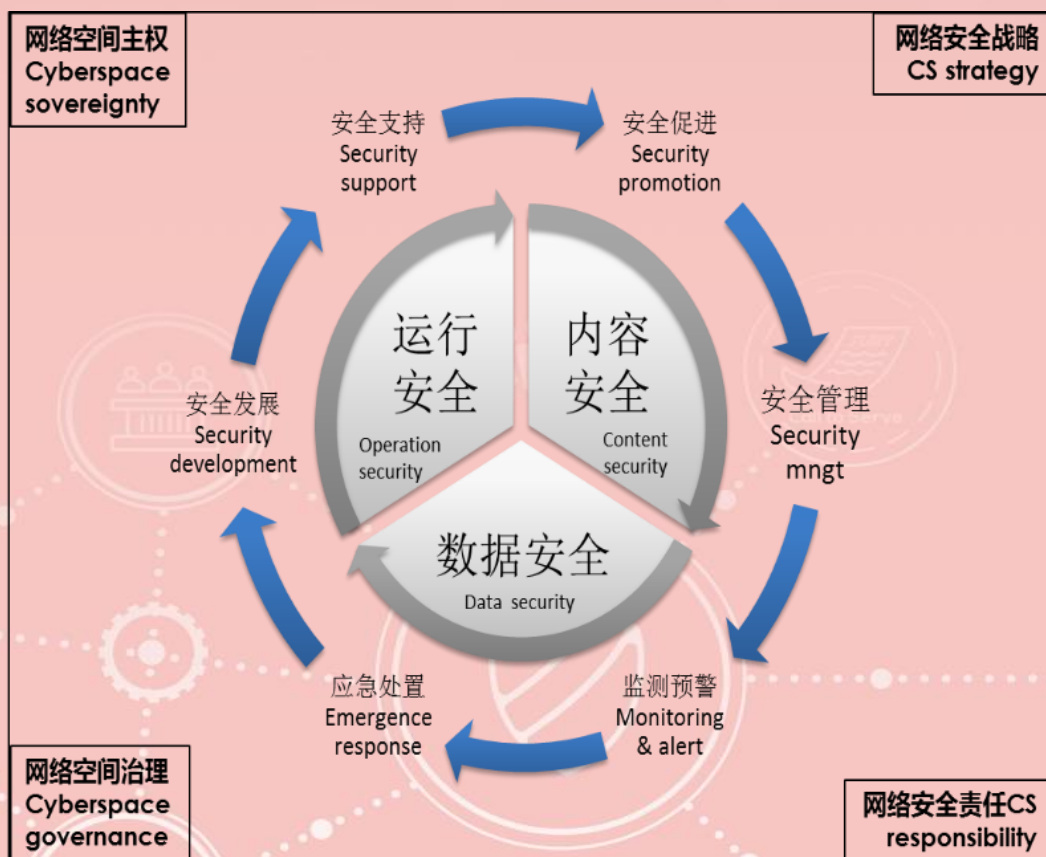
•CSL contents

- C 1 General
- 第二章 网络安全支持与促进
- C2 CS support & promotion
- 第三章 网络运行安全
- C3 Network operation security
 - 第一节 一般规定
 - S1 General provisions
 - 第二节 关键信息基础设施的运行安全
 - S2 CII operation security
- 第四章 网络信息安全
- C4 Network info security
- 第五章 监测预警与应急处置
- C5 Monitoring, alert & emergency response
- 第六章 法律责任
- C6 Legal liability
- 第七章 附则
- C7 Supplementary Provisions



网络空间主权
Cyberspace
sovereignty

网络安全战略
CS strategy



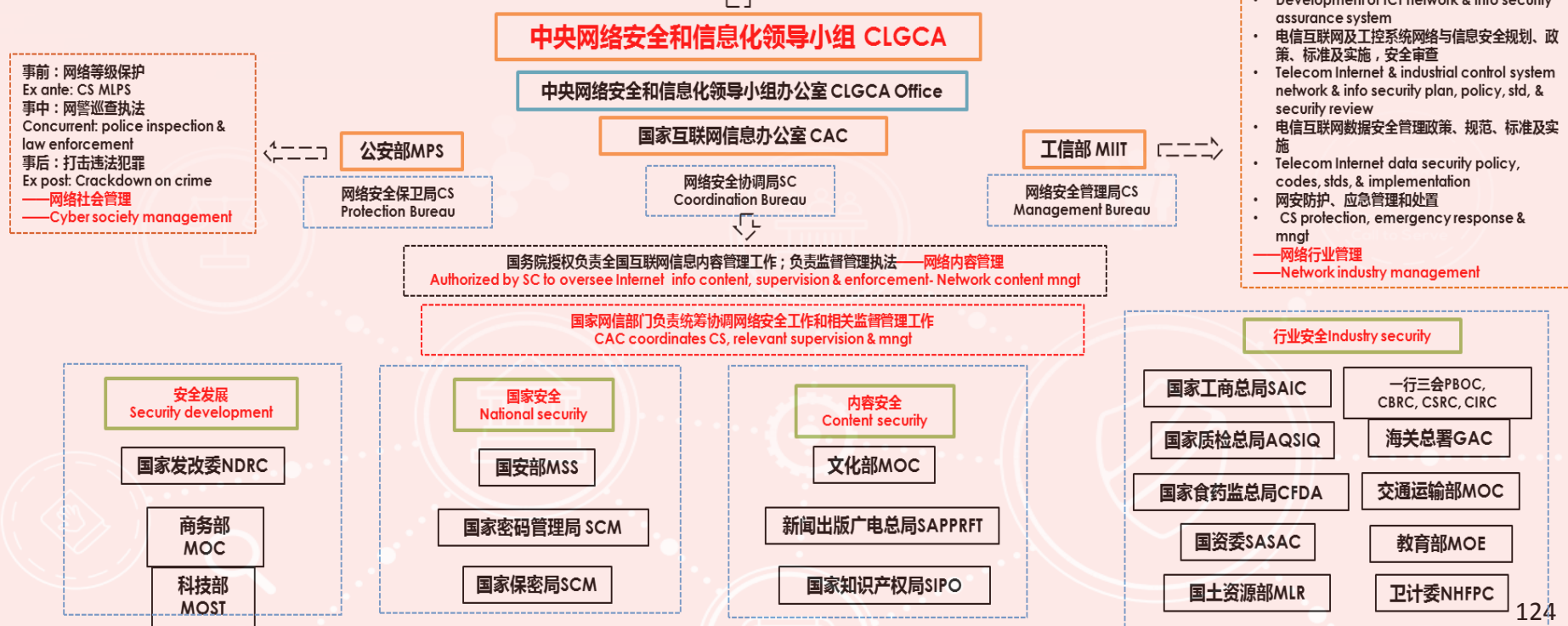
网络空间治理
Cyberspace
governance

网络安全责任
CS
responsibility

Source: Dr. HONG Yanqing, Senior Fellow, Internet Development Research Institute, Peking University

123

统筹协调各领域网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策推动国家网络安全和信息化法治建设，不断增强安全保障能力 Coordinate major CS & info issues in all fields, develop CS & info strategy, broader plans, major policies to drive rule of law over CS & info, to lift security assurance capability

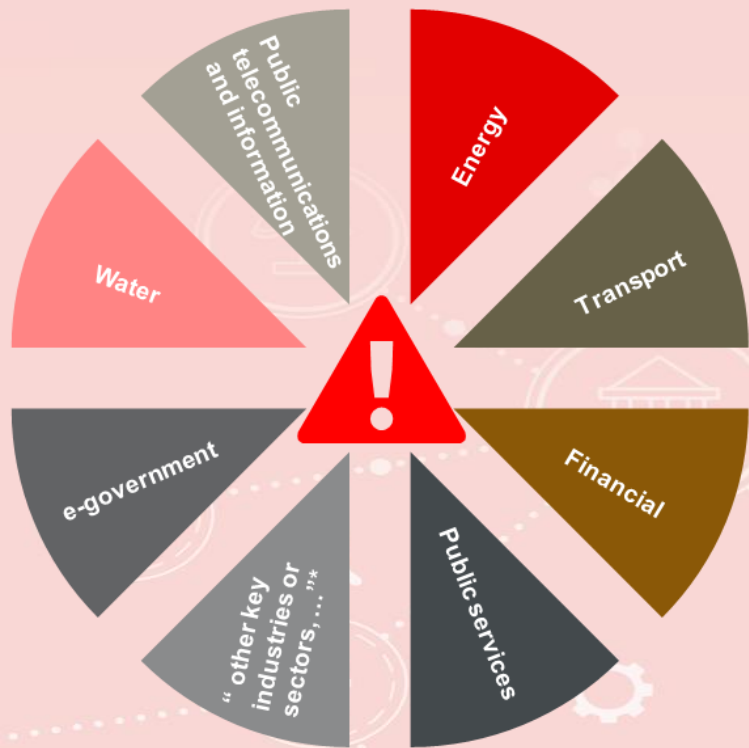


- 电信互联网网络与信息安全技术平台的建设和使用管理
 - Development, use, mngt of telecom Internet network & info security tech platform
 - 信息通信领域网络与信息安全保障体系建设
 - Development of ICT network & info security assurance system
 - 电信互联网及工控系统网络与信息安全规划、政策、标准及实施，安全审查
 - Telecom Internet & industrial control system network & info security plan, policy, std, & security review
 - 电信互联网网络安全管理政策、规范、标准及实施
 - Telecom Internet data security policy, codes, stds, & implementation
 - 网安防护、应急管理和处置
 - CS protection, emergency response & mngt
- 网络行业管理
—Network industry management

- 事前：网络等级保护
Ex ante: CS MLPS
- 事中：网警巡查执法
Concurrent: police inspection & law enforcement
- 事后：打击违法犯罪
Ex post: Crackdown on crime
- 网络社会管理
—Cyber society management

Source: Dr. HONG Yanqing, Senior Fellow, Internet Development Research Institute, Peking University

CII and Data Localisation



Critical Information Infrastructure

- Financial, energy, telecom and information services, water, transportation, e-government
- AND “OTHER KEY INDUSTRIES**”
- PERSONAL DATA and IMPORTANT DATA collected/generated in China
- Stored within the territory of China
- Export of data only allowed for business necessity and pass security assessment

*“other key industries or sectors, which can seriously harm national security or public interest, if destroyed or tampered with or if data is leaked”

125

Source: Barbara Li, Partner of Norton Rose Fulbright LLP Beijing Office

Cybersecurity Law's Major Articles on Data

Data Security 数据安全

Article 10: In construction or operation of networks or supply of services through networks, technical measures and other necessary measures shall be taken.....and **maintain the integrity, confidentiality and availability of network data.**

第10条：“维护网络数据的完整性、保密性和可用性”

Article 21: The State shall implement a cybersecurity multi-level protection system (cyber-MLPS). Network operators shall perform the following security protection duties **to prevent network data leaks, theft or falsification**

第21条：“防止网络数据泄露或者被窃取、篡改”

Article 27: Individuals and organizations must not engage in illegal intrusion into the networks of other parties, disrupt the normal function of the networks of other parties, **or steal network data** or engage in other activities endangering cybersecurity

第27条：“不得提供专门用于……窃取网络数据等危害网络安全活动的程序,工具”

Article 31: The State implements key protection of public communication and information services, power, traffic, water resources, finance, public service, e-government, and other **critical information infrastructure** that if destroyed, loses function, or experiences leakage of data might seriously endanger national security, national welfare and the people’s livelihood, or the public interest

第31条：“一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施”

126

Source: Dr. HONG Yanqing, Senior Fellow, Internet Development Research Institute, Peking University



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

Cybersecurity Law's Major Articles on Data

<p>Protection of Personal Data 个人信息保护</p>	<p>See Further Analysis Below 第40至44条</p>
<p>Data Protection at the State Level 国家层面的数据保护</p>	<p>Article 37: Personal information and important data gathered or produced by critical information infrastructure operators during operations within the territory of the People’s Republic of China, shall store it within the territory of China. 第37条：“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。”</p>
	<p>Article 51: The State cybersecurity and informatization departments shall do overall coordination of relevant departments to strengthen collection, analysis and reporting efforts for cybersecurity information. 第51条：“国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作”</p>
	<p>Article 52: Departments responsible for critical information infrastructure security protection efforts shall establish and complete that industry or that sector's cybersecurity monitoring, early warning and information reporting systems, and report cybersecurity monitoring and early warning information in accordance with regulations. 第52条：“负责关键信息基础设施安全保护工作的部门，应当……按照规定报送网络安全监测预警信息”</p>

Source: Dr. HONG Yanqing, Senior Fellow, Internet Development Research Institute, Peking University



Cybersecurity Law on Personal Information

Cybersecurity Law of China	OECD	GDPR
<p>Article 40 Network operators shall keep the user information they have collected strictly confidential and establish and improve user information protection system.</p>	<p>Accountability Principle</p>	<p>Accountability</p>
<p>Article 41 When collecting or using the personal information, network operators shall comply with the principles of lawfulness, justification and necessity, publicize the rules for collection and use, clearly indicate the purposes, methods and scope of the information collection and use, and obtain the consent of those from whom the information is collected.</p> <p>A network operator shall not collect the personal information irrelevant to the services it provides or collect or use the personal information in violation of the provisions of laws and administrative regulations and the agreements between both parties and shall process the personal information it has stored in accordance with the provisions of laws and administrative regulations and the agreements with the user.</p>	<p>Openness principle</p> <p>Purpose specification principle</p> <p>Collection limitation principle</p> <p>Use limitation principle</p>	<p>Transparency</p> <p>Purpose limitation</p> <p>Data minimisation</p> <p>Lawfulness, fairness</p>

Source: Dr. HONG Yanqing, Senior Fellow, Internet Development Research Institute, Peking University

128



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

Cybersecurity Law on Personal Information

Cybersecurity Law of China	OECD	GDPR
<p>Article 42 Network operators shall not divulge, tamper with or damage the personal information they have collected; they shall not provide such personal information to others without consent of those from whom the information is collected, except for the information that has been processed and cannot be recovered and through which no particular individual may be identified.</p> <p>Network operators shall take technical measures and other necessary measures to ensure the security of the personal information they have collected and prevent the personal information from being divulged, damaged or lost. When the personal information is or might be divulged, damaged or lost, they shall take remedial measures immediately, notify the users in a timely manner in accordance with relevant provisions and report the same to relevant competent authorities.</p>	<p>Use limitation principle</p> <p>Security safeguards principle</p>	<p>Lawfulness, fairness</p> <p>Integrity and confidentiality</p> <p>Mandatory breach notification</p>

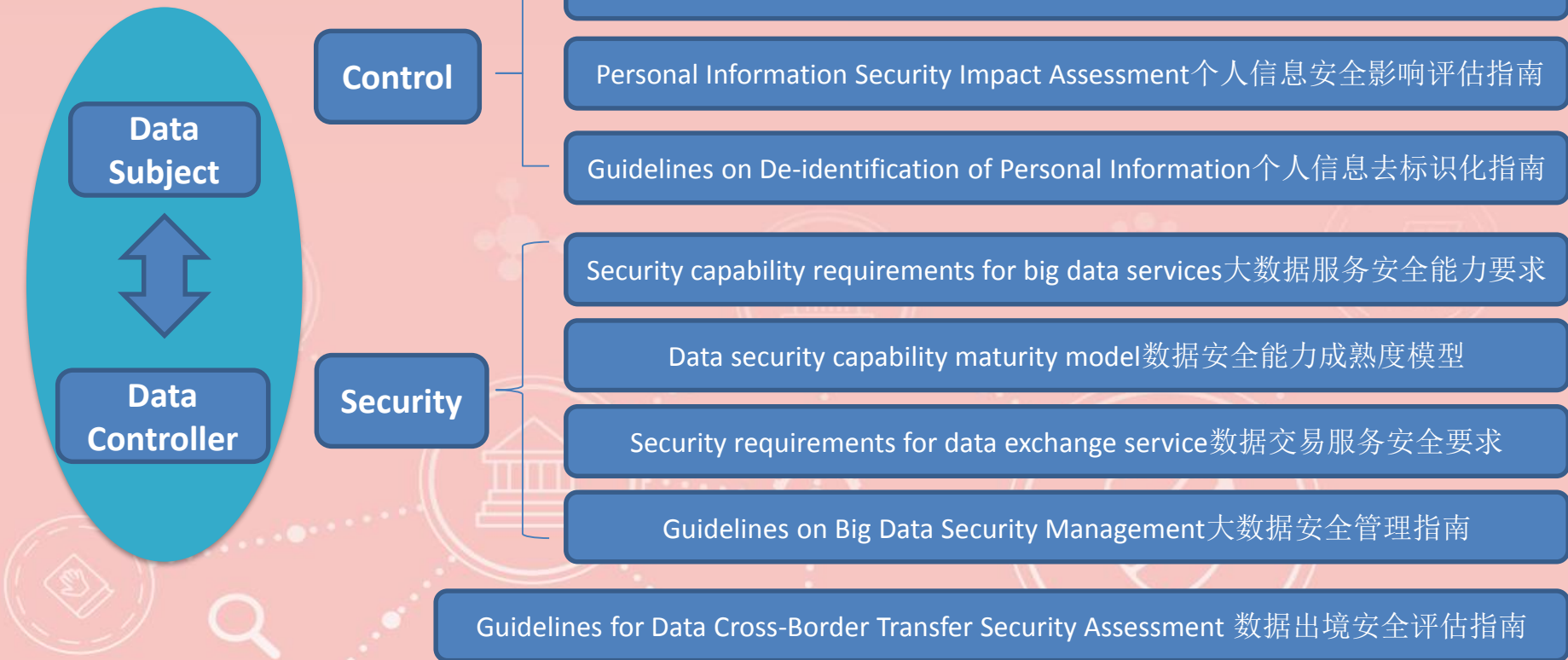
Source: Dr. HONG Yanqing, Senior Fellow, Internet Development Research Institute, Peking University

129

Cybersecurity Law on Personal Information

Cybersecurity Law of China	OECD	GDPR
<p>Article 43 If any person finds that a network operator collects or uses his/her personal information in violation of the provisions of laws and administrative regulations or the agreements between both parties, the person shall have the right to require the network operator to delete his/her personal information; if the person finds that his/her personal information collected or stored by the network operator is erroneous, the person shall have the right to require the network operator to make correction. The network operator shall take measures to delete or correct such information.</p>	<p>Individual participation principle</p>	<p>Right to erasure</p> <p>Right to rectification</p>
<p>Article 44 No individuals or organizations may steal or otherwise illegally obtain the personal information or illegally sell or provide the personal information to others.</p>	<p>Use Limitation Principle</p>	<p>Lawfulness, fairness</p>

Standards Family



Source: Dr. HONG Yanqing, Senior Fellow, Internet Development Research Institute, Peking University

131

	Hong Kong	Mainland
Data Breach Notification	<p>No such requirement under PDPO</p> <p>The Privacy Commissioner encourages data users to report data breaches to the relevant regulatory / law enforcement authorities, and to notify the affected individuals</p>	<p>Cybersecurity Law (網絡安全法)</p> <ul style="list-style-type: none"> To notify user promptly and report to related supervising authority in the event of any security incident or suspected security incident concerning personal information <p>Personal Information Security Specification (個人信息安全規範) (2020 ver.)</p> <ul style="list-style-type: none"> To establish a personal information security emergency response plan To organise regular (at least once a year) emergency response trainings and drills for responsible officers To report and notify the affected data subjects promptly after data breaches

Profiling and Automated Decision-making

No such requirement under PDPO

However, **sections 30-32 of the PDPO** govern “**matching procedure**”, which may be used in conducting profiling

A “**matching procedure**” is one that satisfies the following 4 criteria:

1. the matching of 2 sets of personal data collected for different purposes respectively
2. the procedure involves 10 or more data subjects
3. the procedure is not executed by manual means
4. the result of the matching procedure may be used immediately or at a later time for the purpose of taking adverse action against the data subjects

Data users shall not carry out a “**matching procedure**” unless the consent of the data subjects or the Privacy Commissioner is obtained

The E-Commerce Law (電子商務法)

- If an e-commerce business provides personalised search results to customers, it must also allow the consumers to switch off the personalised recommendations function.

Personal Information Security Specification (個人信息安全規範) (2020 ver.)

- When displaying personalised contents
 - distinguish prominently personalised and non-personalised contents
 - provide consumers the option to cease showing personalized contents
- Before the implementation which has significantly impacts on the rights and interests of the data subjects:
 - conduct a personal information security impact assessment
 - given data subjects an avenue to request reviews of such automated decisions

133

	Hong Kong	Mainland
Enforcement Authority	The Privacy Commissioner	<p>No single dedicated enforcement authority</p> <p>Depending on the industry and the nature of the case, the enforcement authority may include the following:</p> <ul style="list-style-type: none"> • Cyberspace Administration of China (中央網絡安全和信息化委員會辦公室 (網信辦)) • Ministry of Public Security (公安部) • Ministry of Industry and Information Technology (工業和信息化部 (工信部)) • other supervising authorities

The Civil Code

- Will take effect on **1 January 2021**
- An amalgamation of existing civil laws sprawls across seven chapters and 1,260 articles

The Code covers (non-exhaustive):

Private
property

Personal
privacy

Marriage
and family

Inheritance

Contracts

Privacy Right and Personal Information Protection Provisions in the Civil Code

Chapter VI (Privacy and Personal Information Protection)

[第六章 隱私權和個人信息保護] of **Book IV** (Personality Rights) [第四篇 人格權]



Protecting private data and personality rights

136

Privacy Rights and Personal Information Protection Provisions In Civil Code



General Provisions

- **Article 110: a person's general right to privacy**
- **Article 111: a general right to protection of personal information.**
- **Article 994 to 1000: various general rights to seek civil liability claims against privacy and personal information related infringement**

Privacy Right and Personal Information Protection Provisions in the Civil Code



Specific Provisions

- **Article 1032: Definitions of privacy rights and privacy.**
- **Article 1033: Specific actions/conduct that will constitute infringement of privacy rights.**
- **Article 1035: Conditions under which processing/handling of personal information are permitted**
- **Article 1036: Exemptions for processing of personal information**
- **Articles 1037-1039: Rights of data subjects and obligations of data processors (including obligations of special bodies and persons)**

Privacy Right and Personal Information Protection Provisions in the Civil Code



Provisions that are issue or industry specific

For example:

- **Art 1030: handling of information by credit agencies**
- **Art 1226: provisions governing the protection of patients' privacy rights and personal information by medical institutions and their medical personnel**

Privacy in the Civil Code



Not allowed without individuals' consent:

Disturbing the peace of other people's private lives through telephone, text message, instant messaging tool, email, leaflets, etc.

Entering, shooting and peeping into other people's private space such as houses, hotel rooms, etc.

Shooting, peeping into, eavesdropping, publicising other people's private activities

Shooting, peeping at private parts of other people

Processing private information of other people

Invading the right of privacy of other people in other ways

140

Examples of Personal Information in the Civil Code

Natural persons' names

Dates of birth

ID numbers

Biologically identified personal information

Addresses

Telephone numbers

Email addresses, etc.

“Email addresses and whereabouts” are not included in the Cybersecurity Law.

Principles of processing personal information



- Obtaining consent
- Publicising the rules of processing the information
- Stating the purpose, method and scope
- No violation of laws or regulations or agreement between the two parties

Exceptions in Chapter Six

No civil liabilities for data processors,
when:

consent by
such natural
person or
his/her
guardian

the information has
been publicised by
such natural person
or other information
which has been
legally publicised

to maintain public
interests or legal
interests of such
natural person

AI Development and Technology's Ethical Application

said Xue Lan, director of the National New Generation Artificial Intelligence Governance Committee, at a forum during the World Artificial Intelligence Conference (WAIC) in Shanghai on 10 July 2020.

“Data governance is a major challenge we are facing in this era, not only in the field of artificial intelligence but also in platforms with more extensive information applications.”

AI Development and Technology's Ethical Application

“Compared to computing power and algorithms, the only dimension where we can narrow the gap [with Western countries] in artificial intelligence is data.”

“It will be a self-defeating act if [regulation] becomes too strict in the use of data.”

said Huang Wei, chief executive of speech recognition and language processing start-up Unisound Intelligent Technology, in a round table discussion at the WAIC.

AI Development and Technology's Ethical Application

“I think we must be smart in legislation, and be sure to monitor different data in different ways.”

“For companies that are using AI to help treat diseases, it will suffocate them if regulation is too restrictive.”

said Zhou Xiang, chief executive of United Imaging Healthcare, a medical imaging systems and equipment company, at the WAIC round table discussion.



AI Development and Technology's Ethical Application

“[Rigid regulation] will be a challenge for companies that only focus on developing the basic AI algorithms.”

“It used to be, for example, banks or internet companies could access data directly, but now it will not be allowed any more. All data sources must be clear and traceable, and a higher bar will be placed when it comes to data legitimacy and boundaries of using it.”

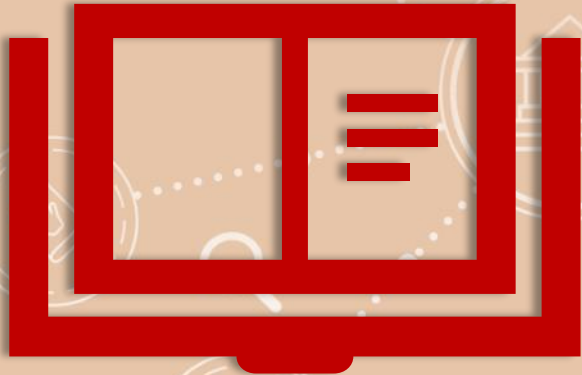
said Sun Lilin, founder and chief executive of Juzix, a privacy computing and blockchain technology services provider

147

The Standing Committee of the NPC is reviewing the draft Data Security Law

Aims:

- protect national security
- promote relevant use of data



PRC Data Security Law (draft)

- covers 51 articles and seven chapters
- focus on national security (Article 1)

The draft Data Security Law provides that national security is the key theme and consideration in formulating and establishment the data security system and related rules.

Applicable Scope

Data Activities

collection

storage

processing

usage

provision

publicity

Electronic forms

non-electronic forms

150

PCPD



PCPD.org.hk

H K

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

Notable Provisions:

Legal liability would be pursued inside and outside of China ...

(Article 2)

... if an entity “engage in data activities that harm the national security, the public interest, or the lawful interests of citizens or organizations.”

Notable Provisions:

A tiered system for data security (Article 19)

A "tiered system" of data security seem to echo with the tiered system of cybersecurity protections (more commonly known as "multiple-level protection scheme") set out in Article 21 of the Cybersecurity Law.

Notable Provisions:

Regional government and sectoral regulators need to producing catalogs of what constitutes “important data” (Article 19)

The catalogs would distribute responsibility widely as to determining the reach of data security responsibilities and requirements.

Notable Provisions:

No specific rules and regulations governing personal information (article 49)

The draft law does not expressly exclude its application on personal information, but it expressly provides that the carrying out of data activities that involve personal information shall comply with relevant laws and regulations.

Local Data Law Amendment Directions

Benefits include:

SEATED FORWARD FOLD (Paschimottanasana)



- Calms the brain and helps relieve stress and mild depression.
 - Stretches the spine, shoulders, hamstrings.
- Stimulates the liver, kidneys, ovaries, and uterus.
 - Improves digestion.
- Helps relieve the symptoms of menopause and menstrual discomfort.
- Soothes headache and anxiety and reduces fatigue.

155

The Change of Global Privacy Landscape

Technology (e.g. AI, Big Data, cloud, IoT, social media) is increasingly making impact on personal data privacy

Many jurisdictions have passed or proposed **new/revised personal data protection law**

The adoption of data protection and privacy legislation **increased by 11%** between 2015 and 2020[#]

66% of nations of the world have data protection legislation[#]



EU GDPR (effective May 2018) raised the benchmark of personal data protection and people's **privacy expectation** to new heights

[#]Source: United Nations Conference on Trade and Development (UNCTAD)

156

Data breach of an airline based in Hong Kong affecting 9.4m passengers

- Suspicious activities on its network detected in March 2018

- Data breach notification not lodged to PCPD until 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

Call for amendment of PDPO

157

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

- I. **Mandatory data breach notification mechanism**
- II. **Requirements on setting out data retention policy**
- III. **Increasing PCPD's sanctioning powers**
- IV. **Regulating data processors directly**
- V. **Clarifying the definition of 'personal data'**
- VI. **Regulation of doxxing**



158

(I) Mandatory Breach Notification Mechanism



Leakage of personal data on the internet is common in information age



Number of data breaches in Hong Kong has been increasing steadily in recent years



No. of data breach notifications received by PCPD reached a **record-high of 139** in **2019**, almost double that in 2014

(I) Mandatory Breach Notification Mechanism



Some data users **took months to voluntarily report a data breach**, falling short of society's expectations



Prompt notifications are important for **mitigating measures** to be taken to prevent further damage



The **global data protection landscape** has moved towards a mandatory breach notification regime

(I) Mandatory Breach Notification Mechanism

Notification threshold

<u>Jurisdiction</u>	<u>Notification Threshold</u>
Australia	“likely to result in serious harm” (for notifying DPA and impacted individuals)
Canada	“ a real risk of significant harm ” (for notifying DPA and impacted individuals)
EU	<u>notifying DPA unless</u> “ <u>unlikely</u> to result in <u>a risk</u> to the rights and freedoms of natural persons” <u>notifying impacted individuals if</u> “likely to result in <u>a high risk</u> to the rights and freedoms of natural persons”
New Zealand	“has caused or is likely to cause serious harm to the impacted individuals” (for notifying DPA and impacted individuals)

(I) Mandatory Breach Notification Mechanism

Notification timeframe

<u>Jurisdiction</u>	<u>Notification timeframe</u>
Australia	'as soon as practicable' (for notifying DPA and impacted individuals)
Canada	'as soon as feasible' (for notifying DPA and impacted individuals)
EU	'without undue delay and, where feasible, no later than 72 hours' (for notifying DPA) 'without undue delay' (for notifying impacted individuals)
New Zealand	'as soon as practicable' (for notifying DPA and impacted individuals)

162

(I) Mandatory Breach Notification Mechanism

Investigation timeframe for suspected breach

<u>Jurisdiction</u>	<u>Investigation timeframe</u>
Australia	Risk assessment is required to be undertaken and completed within 30 days of a suspected data security incident

(I) Mandatory Breach Notification Mechanism

Consequences for failure to make notification

<u>Jurisdiction</u>	<u>Consequences</u>
Australia	Civil penalties up to AU\$2.1 million
Canada	Criminal fine up to CA \$100,000 imposed by court
EU	Fines up to €10 million or 2% of the organisation's total worldwide annual turnover, whichever is higher
New Zealand	Criminal fine of up to NZ\$10,000 imposed by court

164

(I) Mandatory Breach Notification Mechanism

- Notify both the **PCPD** and the **impacted individuals**
- Notification threshold – “***real risk of significant harm***”
- Set **time limit** – e.g. 5 business days for notifying PCPD
- May allow for investigation period for ‘suspected breach’ before notification (e.g. 30 days)
- PCPD may direct data user to notify impacted individuals
- Failure to make notification may result in administrative fine imposed by PCPD.

(II) Additional regulation on retention of personal data

Current provisions:

Data Protection Principle 2:

Personal data is **not kept longer than is necessary** for the fulfilment of the purpose for which the data is or is to be used

Does not define when personal data is “no longer necessary”

No fixed retention period requirements

No requirements for setting data retention policy

But there is no one-size-fit-all approach to data retention

Data retention – Overseas provisions

Generally do not spell out the definite retention period for personal data:

EU GDPR: Personal data kept **no longer than necessary**

Canada PIPEDA: ...personal data shall be retained **only as long as it is necessary** for the fulfilment of the collection purposes

Australia APA: ...destroy the personal data that the entity **“no longer needs”** for the allowed purposes

New Zealand NZPA: **“shall not keep [personal data] for longer than is required”** for the purposes for which the information may lawfully be used

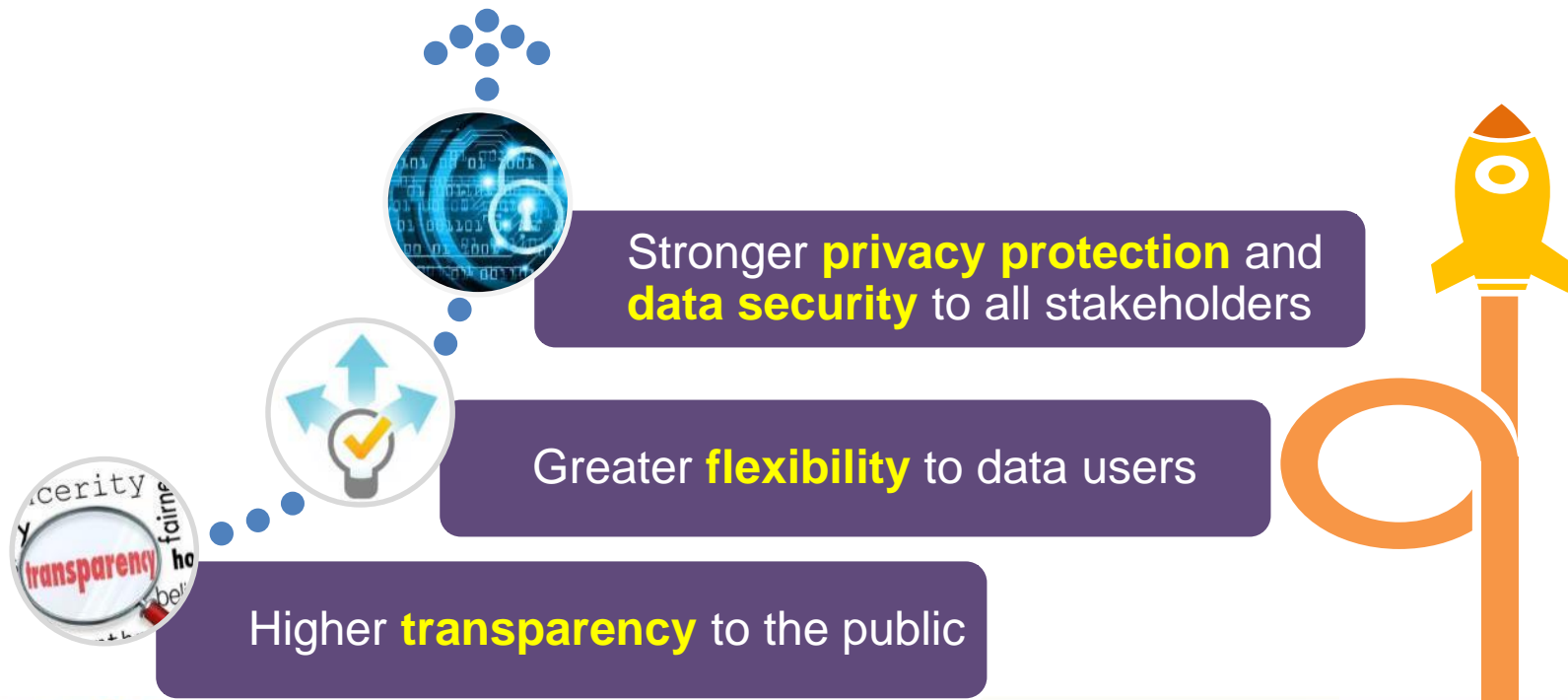
Singapore PDPA: cease to retain personal data **“as soon as it is reasonable”** [...] **“no longer necessary”** for any legal, business or other collection purposes

167

(II) Additional regulation on the retention of personal data

- Amend DPP5(a) to expressly include the retention policy in the information to be made available
- Data users to formulate and disclose personal data **retention policy**
- Disclose **maximum retention** period for different categories of personal data

Data retention policy – A well-balanced direction



169

(III) PCPD's Sanctioning Powers

Existing Issues



PCPD has no authority to impose administrative fines, or carry out criminal investigation and prosecution



Current penalty provisions in the PDPO:

- Contravention of DPPs is not an offence
- PCPD may issue an enforcement notice, non-compliance with which is a criminal offence
- Offences under S.64 (e.g. criminal doxxing) and Part 6A (direct marketing) may attract higher penalties



Penalty levels may not reflect the seriousness of the offence and the harm suffered by affected data subjects:

- From 1996 to June 2020: only 35 cases resulted in conviction by court (mostly direct marketing-related), fines imposed were all relatively low

PDPO criticised for its weak deterrent effect

(III) PCPD's Sanctioning Powers



Not uncommon for local and overseas non-judicial bodies to have the power to impose monetary penalties

Overseas examples:
EU Data Protection Authorities
[@GDPR]; UK ICO [@DPA 2018];
Singapore PDPC [@PDPA]

Local examples:
Hong Kong Monetary Authority;
Securities and Futures
Commission

Administrative fine is an effective and efficient alternative to criminal prosecution

Less onerous legal requirements than criminal court proceedings

More expeditious and cost-effective enforcement tool

Less stigma than criminal conviction by court

(III) PCPD's Sanctioning Powers

- Confer additional powers on the PCPD to impose **administrative fines**
- Maximum level of fine may be a **fixed amount or a percentage of the annual turnover**, whichever is higher
- Administrative fines **credited to the HKSAR Government** and not the coffers of the PCPD

Procedures for imposing administrative fines

Recommendations alleviating concerns that the PCPD may arbitrarily impose administrative fine:

- **Procedure** – The PCPD to provide an **administrative fine notice** to the data user or data processor of its intent to impose an administrative fine, the circumstances of any breach, the investigation findings and the indicative level of fine, along with a rationale for the fine.
- **Right to representation** – Upon receipt of the aforesaid notice, the data user or data processor should be given no less than **21 calendar days to make representation**.
- **Right to appeal against the administrative fine notice** – once an administrative fine notice is issued to a data user or data processor, it has the **right to appeal to court** or the Administrative Appeals Board against the notice within **28 calendar days**.

(IV) Regulate data processors directly

Existing Issues

Outsourcing data activities are becoming more common

The PDPO does not regulate data processors

Data processor acting purely on behalf of an overseas data user is not subjected to regulatory oversight of PDPO, i.e. PCPD cannot investigate breaches of DPPs. ❌

The apportionment of responsibility between data users and data processors is often unclear, resulting in insufficient data protection. ❌

Hong Kong's reputation as a regional or international data centre is compromised if the PCPD has no *locus standi* to investigate data security incidents involving processors (e.g. cloud service providers). ❌

(IV) Regulate data processors directly

Many **overseas regulatory models** adopt direct regulation on data processors:

Australia APA, Canada PIPEDA, New Zealand NZPA:
Both data user and processor are directly regulated

EU GDPR, Singapore PDPA:
Data processors directly regulated and indirectly regulated through data users

(IV) Regulate data processors directly

Direct regulation of data processors can...

Eliminate legal loopholes in existing provisions

Ensure **fair share of responsibilities** between data users and data processors

Enhance protection for personal data during processing

Improve the cloud readiness and reputation of Hong Kong by attaining a **satisfactory regulatory environment**

176

(IV) Regulate data processors directly

Data processors' obligations on:

- **retention period** of personal data
- **security** of personal data
- **notification to data users and PCPD** of data breaches without undue delay

(V) Clarify the definition of ‘personal data’

Existing Issues

The concept of “personal data” under the PDPO has been challenged by ICT developments

PDPO currently only applies to data that can be practicably used to ascertain the identity of a person

New technologies causing new privacy concerns

E.g. Metadata and IP address are not ‘personal data’ under PDPO, but they could be used to conduct profiling

Many overseas judicial authorities extended their data protection regimes to cover IP address and other online identifiers

E.g. EU’s GDPR

Definitions of “personal data”

PDPO	Overseas (e.g. AU, CA, EU)
Criteria: <ul style="list-style-type: none">• Practicable to <u>ascertain identity</u>	Criteria: <ul style="list-style-type: none">• Relating to or about an <u>identifiable</u> individual
Meaning: <ul style="list-style-type: none">• <u>Knowing</u> who a person is	Meaning: <ul style="list-style-type: none">• Able to <u>single out</u> a person, not necessarily knowing who the person is
Result: <ul style="list-style-type: none">• <u>Narrower</u> scope of personal data and <u>less</u> protection to privacy	Result: <ul style="list-style-type: none">• <u>Wider</u> scope of personal data and <u>stronger</u> protection to privacy

(V) Expand the definition of ‘personal data’

Personal data may include:

- Information practicable to ***ascertain an identity*** (direct/indirect); and
- Information ***relating to an identifiable*** person

Large scale criminal doxxing incidents

Existing Issues

- Around **5,000** doxxing cases since June 2019
- Current provisions: It is an offence to disclose any personal data of a data subject which was obtained from a data user without the data user's consent and if the disclosure causes psychological harm to the data subject. (Section 64(2))



DOXXING

181



(VI) Regulation of doxxing

- Introduce legislative amendments to specifically address doxxing
- Confer on the Privacy Commissioner statutory powers to:
 - ✓ Compel the **removal of doxxing contents** from platforms/websites
 - ✓ Carry out **criminal investigation and prosecution**



MOUNTAIN POSE (Tadasana)



RegTech

Benefits include:

- Improves Posture
- make you feel stronger
- increase blood circulation
- reduce tension
- help you feel refreshed

Market of Privacy Management Software in 2020

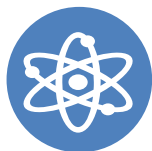
Growth of the Privacy Technology Marketplace



(Source: IAPP 2020 Privacy Tech Vendor Report)

Examples of Privacy Management Software

Consent Manager



Website Scanning

**Assessment
Manager**



**Data Discovery and
Data Mapping**



**Data Subject
Requests**



Consent Manager

Integrate with users' data collection platform



Manage the entire consent lifecycle, from collection through withdrawal



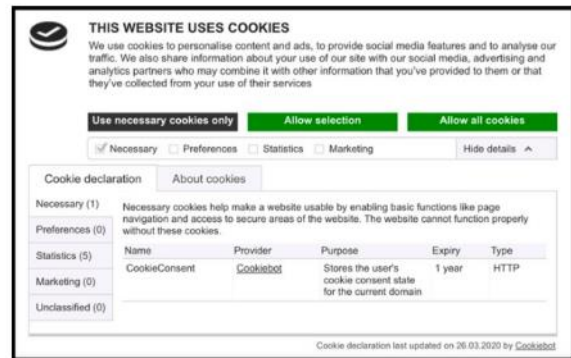
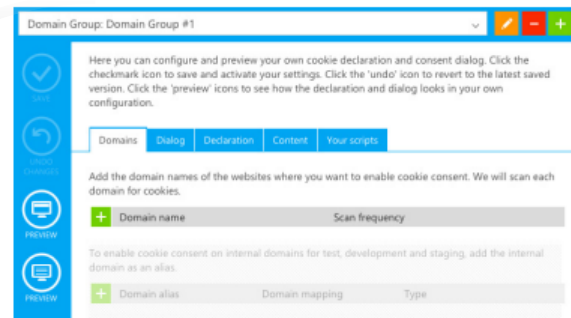
Maintain central database of consent



Create consent banner, declaration & opt-out for compliance



Collect valid user's consent



(Source: Cookiebot)

186

Data Discovery & Data Mapping

Survey systems to identify where personal data reside



Automatically classify personal data according to predetermined criteria



Create data mapping to visualise the flows of personal data, both within and outside organisations



Generate real time, up-to-date records of processing activities



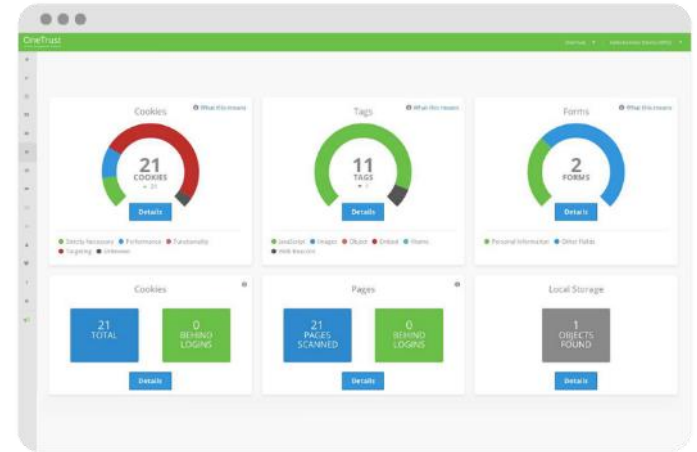
(Source: AvePoint, TrustArc)

Website scanning

Scan websites to determine what cookies, beacons and other tracker are embedded



Ensure compliance with various cookies laws and other regulations



(Source: OneTrust)

Assessment Manager



(Source: TrustArc)

Data Subject Requests

Quickly verify the requestor identity to validate requests



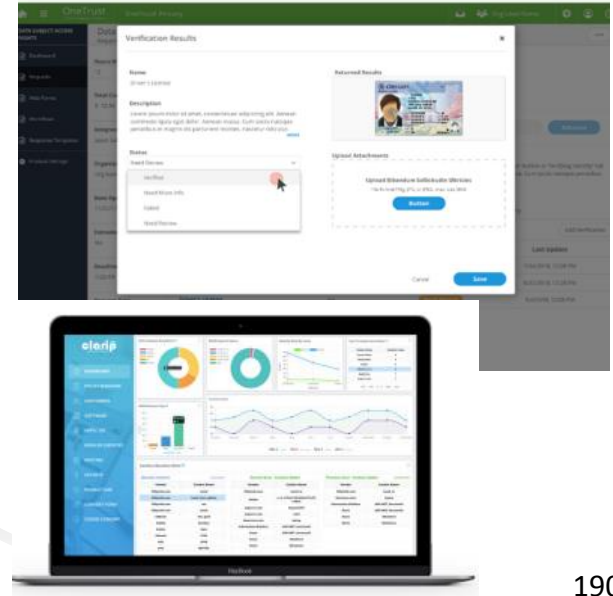
Streamline the process by utilising templates



Execute user requests timely and accurately



Maintain comprehensive records



(Source: OneTrust, Clarip)

190

JOIN

Data Protection Officers' Club

(Membership Application)



保障資料主任聯會
DATA
PROTECTION
OFFICERS'
CLUB

By becoming a DPOC member, you will:

- advance your knowledge and practice of data privacy compliance through experience sharing and training;
- enjoy 20% discount on the registration fee for PCPD's Professional Workshops;
- receive updates on the latest development in data privacy via regular e-newsletter

As a DPOC member, your organisation's name will be published on DPOC membership list at PCPD's website, demonstrating your commitment on personal data protection to your existing and potential customers as well as your stakeholders.

Membership fee: HK\$350 per year
Enquiries: d poc@pcpd.org.hk

[https://www.pcpd.org.hk/
misc/dpoc/enrol.html](https://www.pcpd.org.hk/misc/dpoc/enrol.html)



Contact Us

www.pcpd.org.hk

