

Cloud Expo Asia, Hong Kong 2018

Hong Kong Convention and Exhibition Centre

16.05.2018

Cybersecurity Law, GDPR and Data Ethics

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

Stephen Kai-yi Wong, Barrister

Privacy Commissioner for Personal Data, Hong Kong

Cloud Computing



Characteristics:

Rapid cross-border data flow

Unknown/little control over data storage locations

Rapidly changing/loose outsourcing arrangements

Standardised contracts adopted by the cloud service providers

Cloud Computing and Personal Data Privacy

Bottom Line



A stylized illustration of a man's face and upper torso. The man has a large, round, light-colored head with a dark mustache and a small, neutral mouth. He is wearing a red and white checkered shirt. He is holding a brown telephone receiver to his ear with his right hand. In the top right corner, there is a thought bubble containing a white download icon. The background is a solid light blue color.

Cybersecurity Law

Mainland's Data Protection Regime



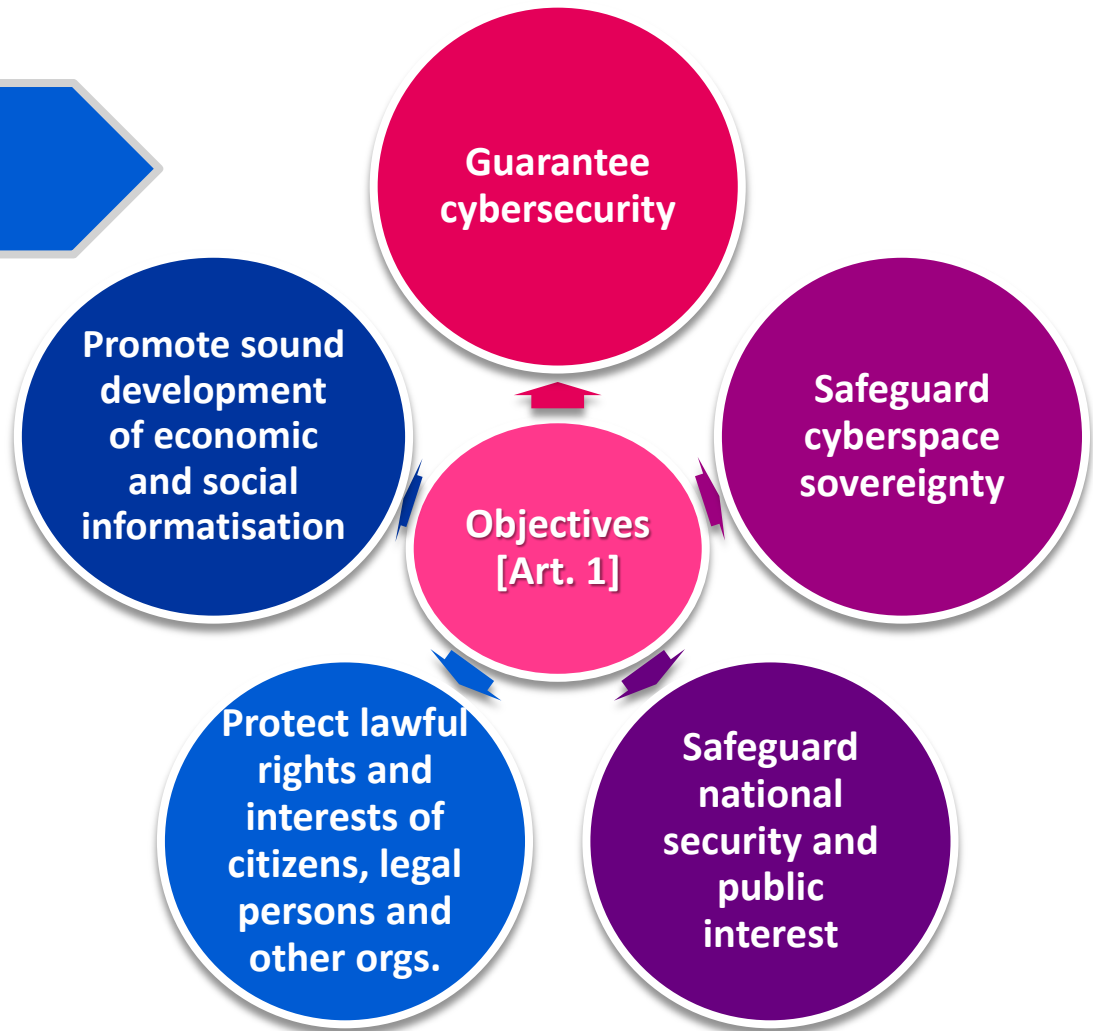
No omnibus data protection law in the mainland of China currently

Personal data privacy protection governed by sectoral law

Hong Kong businesses with interests in the mainland of China should closely monitor recent developments to prepare for compliance

Mainland's Cybersecurity Law

- Effective on 1 June 2017
- Does not apply in HK

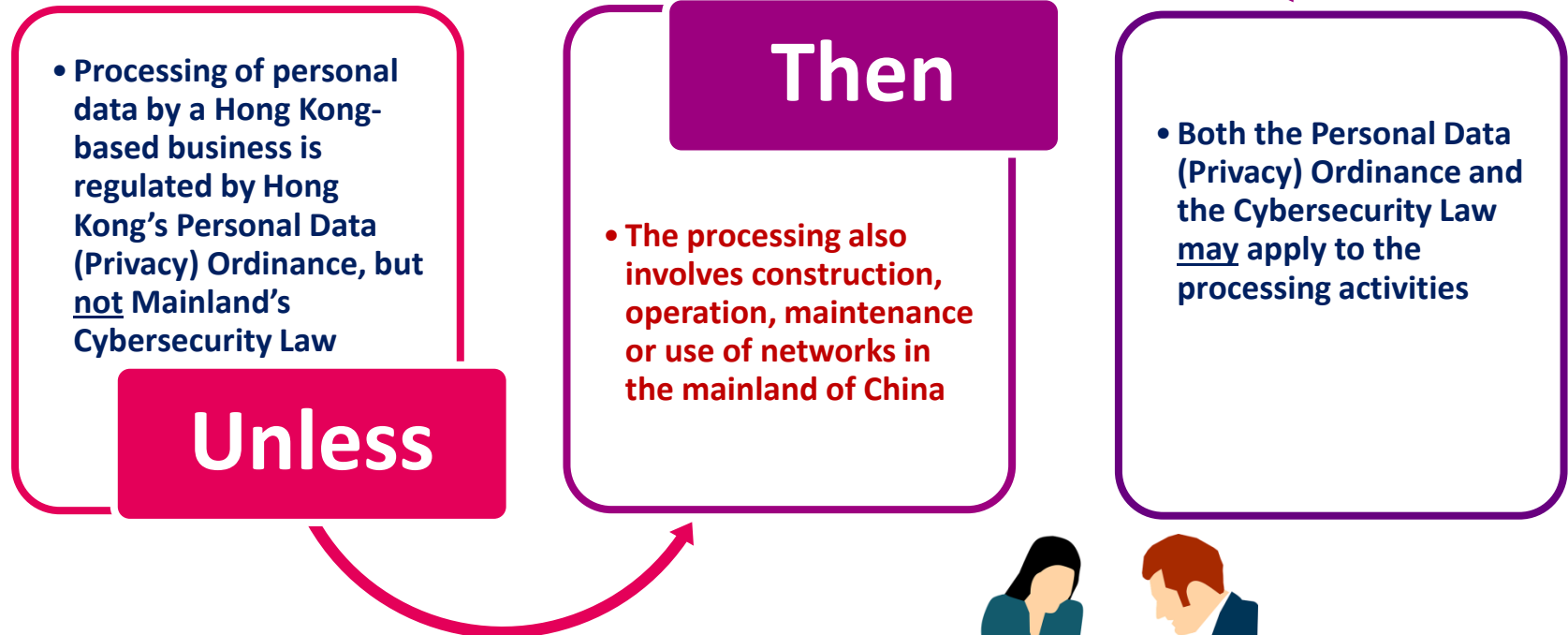


Mainland's Cybersecurity Law

Scope of Application:

- Apply to the construction, operation, maintenance and use of **networks**, and the supervision and administration of **cybersecurity** within China [Art. 2]
- Regulate **network operators**, i.e. owners and administrators of networks, and network service providers [Art. 76(3)]
- Protect **personal information**

How May Cybersecurity Law Affect Hong Kong Businesses?



Comparison between Cybersecurity Law and PDPO



Collection & Use

Cybersecurity Law

Art. 41 (collection & use)

- Follow the principles of **lawfulness, propriety** and **necessity**
- Obtain **consent** from data subjects
- **Do not collect** personal information **irrelevant** to services provided
- Disclose related policy and practice
- Clearly indicate the **purposes, means** and **scope** of collection and use
- **Do not collect or use** personal information **in violation** of agreements with the data subjects

Art. 42 (disclosure)

- Personal information shall not be disclosed to third parties without the data subject's consent

HK PDPO

DPP1 (collection)

- No consent requirement
- Collect data in a lawful and fair way, for a purpose directly related to a function or activity of the data user
- Data collected shall be necessary but not excessive
- Notify data subjects about the purpose of collection, the classes of persons to whom the data may be transferred, and the contact person

DPP3 (use, including disclosure)

- Shall not use personal data for new purposes, unless with prescribed consent of data subjects

Comparison between Cybersecurity Law and PDPO



Security & Data Breach Notification

Cybersecurity Law

Art. 42 (security & notification)

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

HK PDPO

DPP4 (security)

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

Comparison between Cybersecurity Law and PDPO



Cross-border Data Transfer

Cybersecurity Law

Art. 37 (data localisation)

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

HK PDPO

S. 33 (prohibition against transfer)

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

What is Critical Information Infrastructure under Cybersecurity Law?

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

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

[Art. 31]



Comparison between Cybersecurity Law and PDPO



Sanctions

Cybersecurity Law

Arts. 64 & 66

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

HK PDPO

- PCPD has no power to impose administrative sanction

Ss. 50 & 50A

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

Information security technology — Personal information security specification

《信息安全技术 个人信息安全规范》

- Implemented on 1 May 2018
- Comprehensive personal data protection standard in mainland China
- Developed with reference to personal data protection guidelines/regulations of OECD, EU and USA
- Recommended good practice – organisations that follow the Specification will be taken to have observed the data protection requirements under the Cybersecurity Law
- Provide guidance for compliance with the data protection principles in the Cybersecurity Law

A stylized illustration of a man's face and upper torso. He has a large, dark grey mustache and is wearing a red and white checkered shirt. He is holding a yellow telephone receiver to his ear. In the top right corner, there is a thought bubble containing a white download icon. The background is a light blue color.

General Data Protection Regulation (GDPR)



PDPO – GDPR Comparative Study


Background

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



PDPO – GDPR Comparative Study

Major differences between PDPO and GDPR:


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

Cloud service providers with customers/clients in the EU should be mindful of the extra-territorial application of GDPR



PDPO – GDPR Comparative Study

Major differences between PDPO and GDPR:


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

Broader definition of personal data under GDPR



PDPO – GDPR Comparative Study


Major differences between PDPO and GDPR:

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



PDPO – GDPR Comparative Study


Major differences between PDPO and GDPR:

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



PDPO – GDPR Comparative Study


Major differences between PDPO and GDPR:

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



PDPO – GDPR Comparative Study


Major differences between PDPO and GDPR:

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



PDPO – GDPR Comparative Study

Major differences between PDPO and GDPR:


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

Cloud service providers are likely to be regarded as data processors to their customers under GDPR



PDPO – GDPR Comparative Study


Major differences between PDPO and GDPR:

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



PDPO – GDPR Comparative Study


Major differences between PDPO and GDPR:

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



PDPO – GDPR Comparative Study

Major differences between PDPO and GDPR:

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


Industry resources:

- **Code of Conduct for GDPR Compliance (issued by the Cloud Security Alliance (CSA) in Nov 2017):** <https://gdpr.cloudsecurityalliance.org/>
- **EU Cloud Code of Conduct (May 2017):** <https://eucoc.cloud/en/home.html>

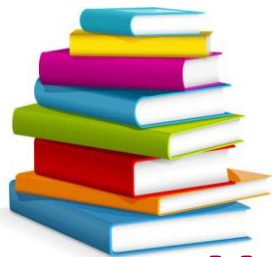


PDPO – GDPR Comparative Study

Major differences between PDPO and GDPR:


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

Cloud service providers may make use of certification mechanism and/or approved codes of conduct for the transfer of personal data out of EU



PDPO – GDPR Comparative Study

Major differences between PDPO and GDPR:

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

“European Union General Data Protection Regulation 2016” Booklet



www.pcpd.org.hk/tc_chi/resources_centre/publications/files/eugdpr_c.pdf



www.pcpd.org.hk/english/resources_centre/publications/files/eugdpr_e.pdf

29

A stylized illustration of a man's face and upper torso. He has a large, round, light-colored head with a dark mustache and a small, downturned mouth. He is wearing a red and white checkered shirt. He is holding a yellow telephone receiver to his ear. In the top right corner, there is a thought bubble containing a white downward-pointing arrow. The background is a light blue color.

Access by Law Enforcement Agencies

United States v Microsoft

(US Supreme Court case)



Implications:

US authorities may compel US-based service providers to provide data stored on the latter's servers, regardless of whether that data is stored in the US or a foreign jurisdiction.

- Must a US provider of email services comply with a US warrant by disclosing electronic communications within its control even if the communications are stored in non-US jurisdictions?
- The case is **moot** due to the passage of the Clarifying Overseas Use of Data Act (**CLOUD Act**) by the US Congress in March 2018.

31

e-Evidence Regulation of the EU



- Proposed by the European Commission on 17 April 2018
- **Objective:** makes it easier and faster for police and judicial authorities to access the electronic evidence (e.g., emails, texts or messaging apps) they need in investigations
- A judicial authority in one Member State can obtain electronic evidence directly from a service provider (or its legal representative) in another Member State, **regardless of the location of data**
- Service providers are obliged to respond within 10 days, and within 6 hours in cases of emergency
- Investigators could also require that certain data not be deleted
- A service provider that offers services in the EU **but without a presence in the EU** is still subject to the same obligations

A stylized illustration of a man's face and upper torso. He has a large, dark grey mustache and is wearing a red and white checkered shirt. He is holding a yellow telephone receiver to his ear. The background is light blue with some orange circular shapes in the top right corner. The text "Accountability & Ethics" is written in a bold, blue, sans-serif font across the center of the image.

Accountability & Ethics

Mishandling of Personal Data

Facebook says data leak hits 87 million users, widening privacy scandal

David Ingram

4 MIN READ

SAN FRANCISCO (Reuters) - Facebook Inc said on Wednesday the personal information of 87 million users, mostly in the United States, may have been improperly shared with political consultancy Cambridge Analytica, up from a previous news media estimate of more than 50 million.



Trust in Facebook has dropped by 66 percent since the Cambridge Analytica scandal

Sixty-five percent of survey respondents say they want Facebook to disclose how it uses the personal information it collects.

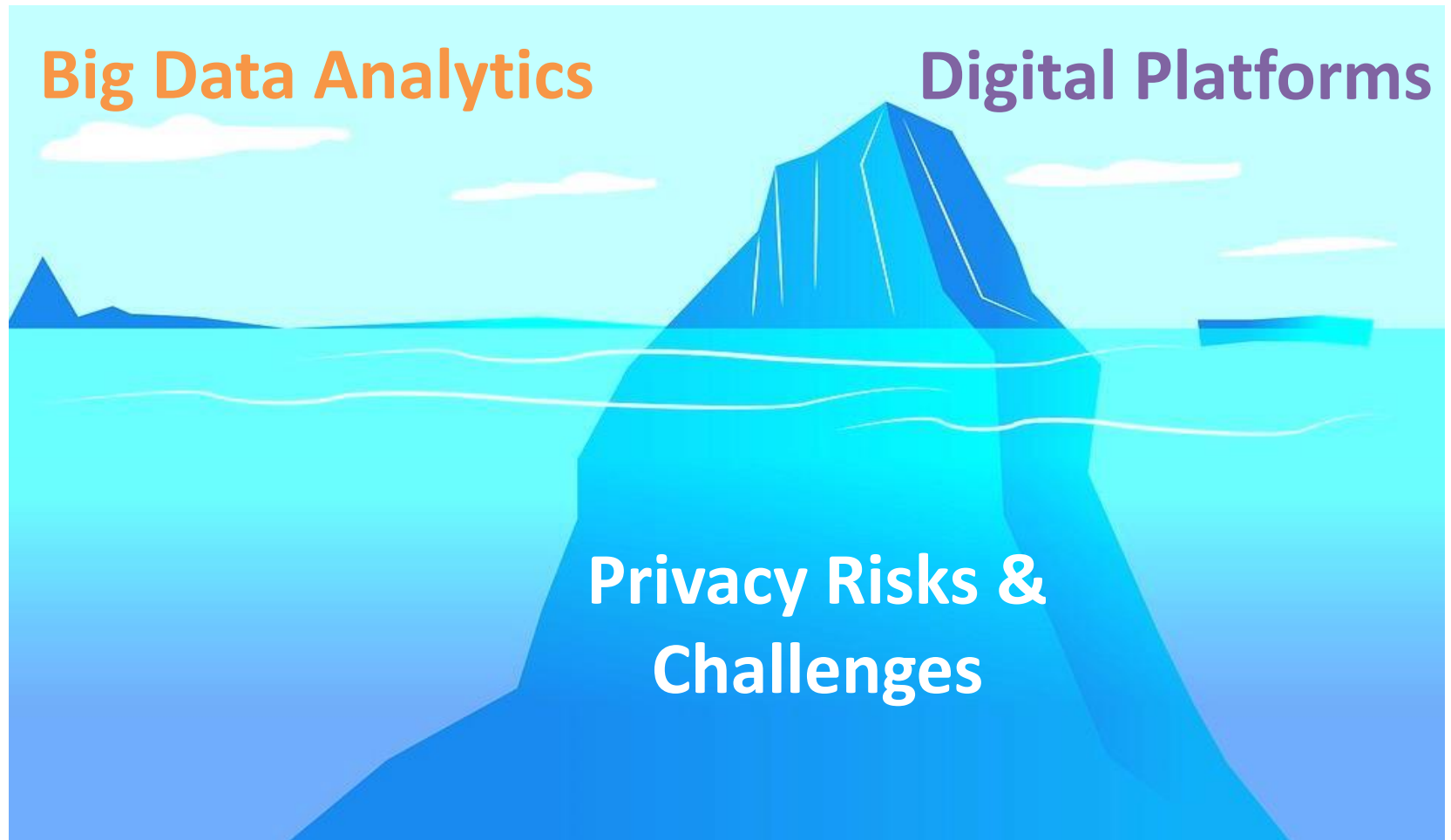
by Herb Weisbaum / Apr. 19, 2018 / 3:08 AM ET



Sources: Reuters; NBC News

34

Privacy Risks and Challenges



Ubiquitous and Covert Data Collection



Data Minimization

Data Transparency



Adequate Notification



Erodes Individuals' Control Over Data

Unpredictable Analytics



X Notice & Consent



X Purpose & Use Limitations

Profiling



Re-identification



✘ Distinction between Personal Data & Non-Personal Data

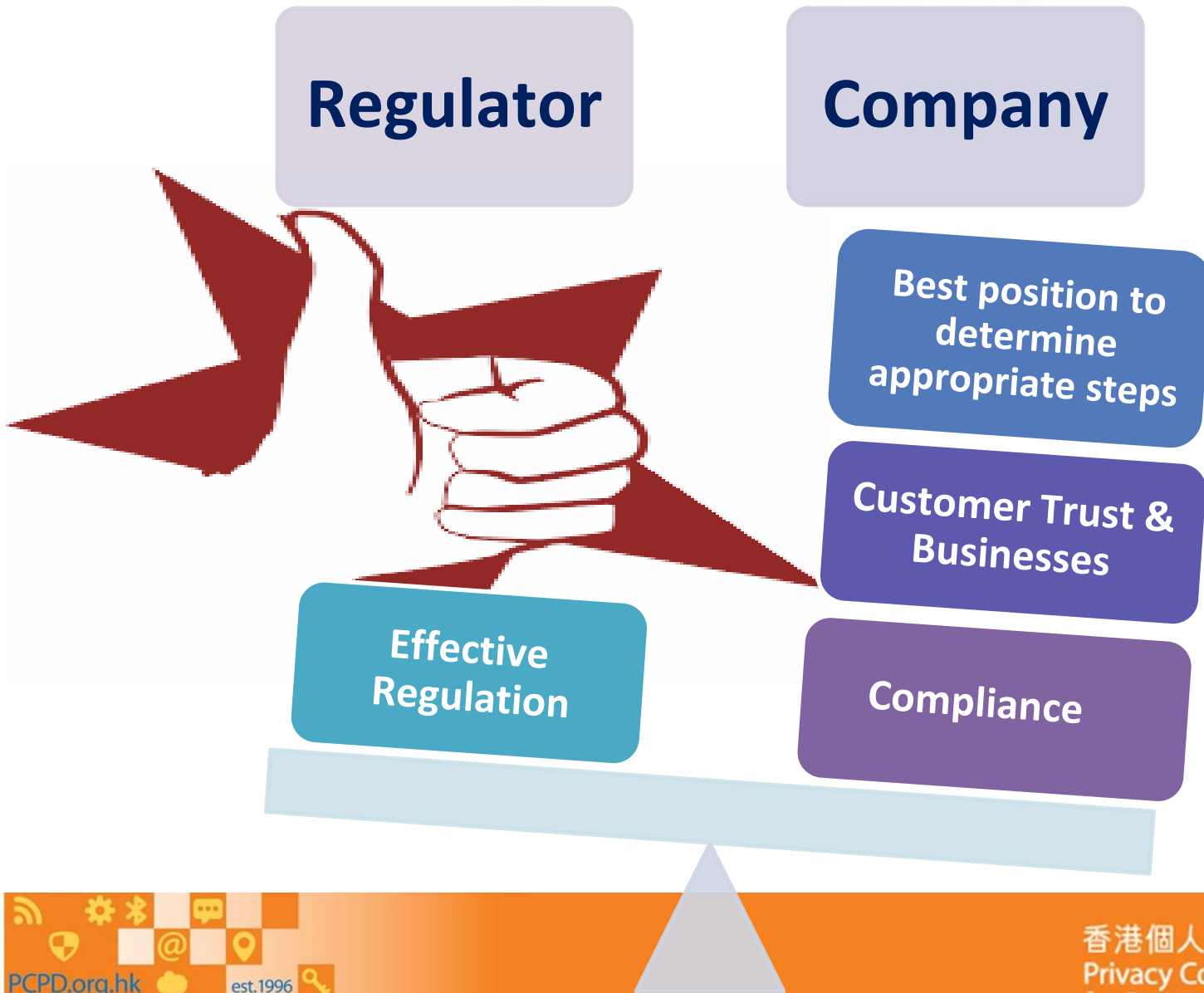
Inaccurate Inferences and Predictions

✗ Data Accuracy

Filter Bubble

Interference in Elections...

Why Accountability?



Mechanics of Accountability

Voluntary/Self-Regulatory

or

Mandatory

Accountability?



Education → Incentivise



Data Ethics and Trust



- No Surprise to Consumers
- No Harm to Consumers

Building Confidence and Trust

Short term actions:

Data users

- Be transparent
- Obtain meaningful consent
- Report data security incidents without delay

Medium and long term actions:

Regulators

- Education
- Fair and proactive enforcement
- Updating the law
- Use of certification & trust marks

Data users

- Paradigm shift from compliance to accountability
- Develop privacy-friendly culture
- Ethical processing of personal data



CONFIDENCE &
TRUST

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

歐洲聯盟
《通用數據保障條例 2016》
小冊子 – 中文版



歐洲聯盟
《通用數據保障條例 2016》
小冊子 – 英文版



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

PCPD.org.hk