ASIAN LEGAL BUSINESS

HONG KONG DATA PROTECTION FORUM

15 November 2017

Challenges of Notice & Consent Model
&
Smart Regulation in Digital Economy

Sandra LIU, Senior Legal Counsel

Privacy Commissioner for Personal Data, Hong Kong

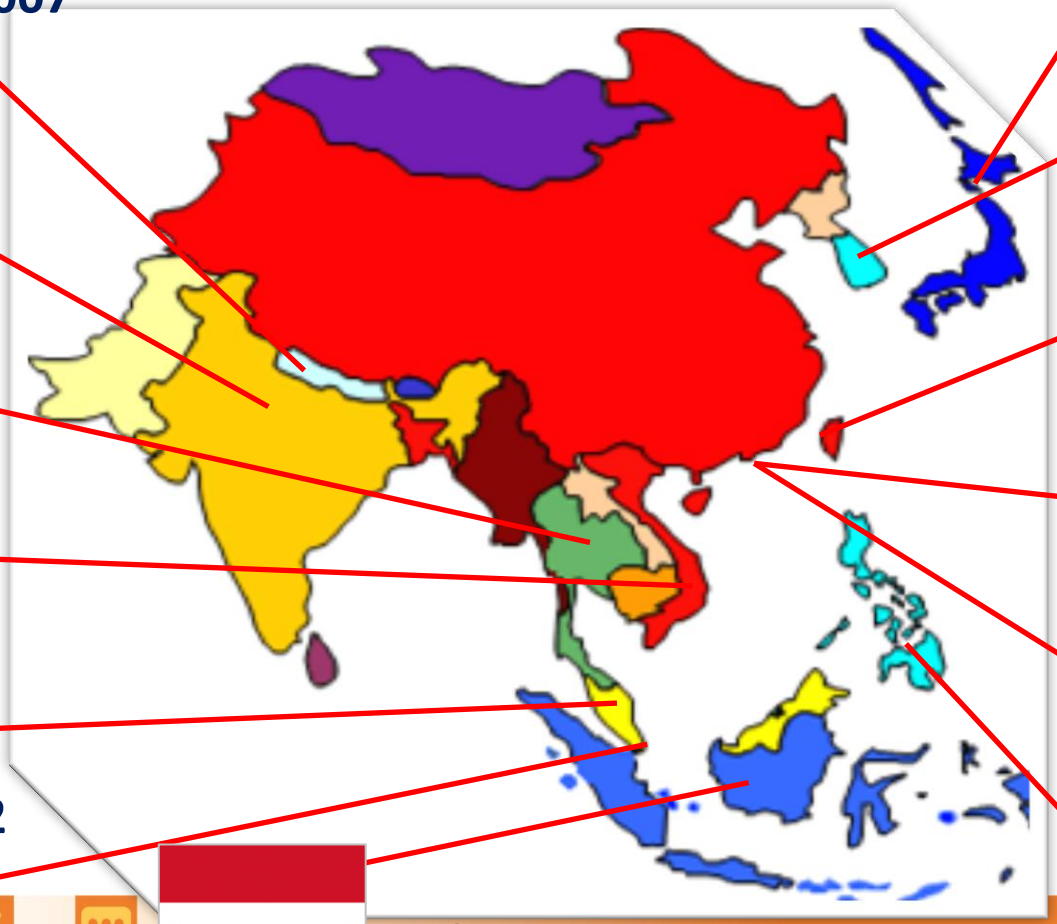
PCPD.org.hk

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

Presentation Outline

- Overview of Personal Data (Privacy) Ordinance
- “Notice” and “Consent” under PDPO
- Positions of OECD Privacy Guidelines and GDPR
- Challenges of Notice & Consent Model
- How to Address the Challenges of Notice & Consent Model in Digital Age
- Smart Regulation in Digital Economy

The Personal Data Protection Landscape in Asia



Nepal - 2007

India - 2011

Thailand - 1997

Vietnam - 2010

Malaysia - 2010

Singapore - 2012

Indonesia - 2016

Japan - 2003

S. Korea - 2011

Taiwan - 2010

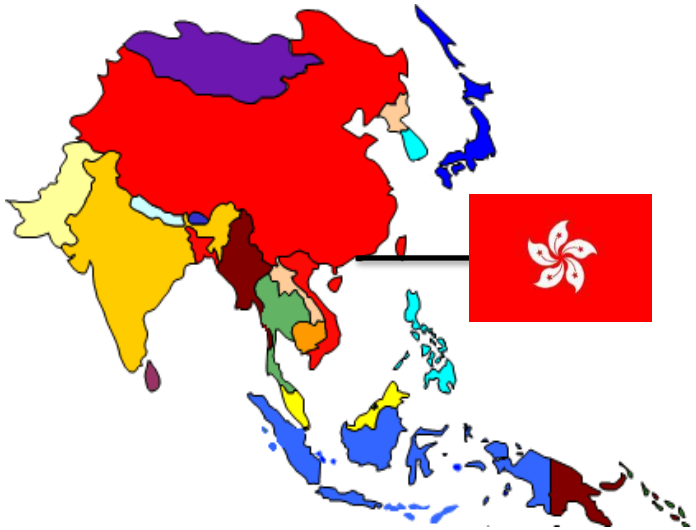
Hong Kong - 1995

Macau - 2005

Philippines - 2012

Personal Data (Privacy) Ordinance

- 1st comprehensive data protection law in Asia
- referenced to 1980 OECD Privacy Guidelines and 1995 EU Data Protection Directive
- covers the public (government) and private sectors
- enforced by an independent statutory regulatory body – the Privacy Commissioner for Personal Data, Hong Kong



Personal Data (Privacy) Ordinance

- enacted in 1995
- core provisions came into effect on 20 December 1996
- Personal Data (Privacy) (Amendment) Ordinance 2012 effective from 1 October 2012 except for "direct marketing" and "legal assistance" provisions which took effect on 1 April 2013

Personal Data (Privacy) Ordinance

6 保障資料原則 Data Protection Principles

PCPD.org.hk

1 收集目的及方式 Collection Purpose & Means

資料使用者須以合法和公平的方式，收集他人的個人資料，其目的應直接與其職能或活動有關。

須以切實可行的方法告知資料當事人收集其個人資料的目的，以及資料可能會被轉移給哪類人士。

收集的資料是有實際需要的，而不超乎適度。

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

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

Data collected should be necessary but not excessive.

2 準確性儲存及保留 Accuracy & Retention

資料使用者須確保持有的個人資料準確無誤，資料的保留時間不應超過達致原來目的的實際所需。

Personal data is accurate and is not kept for a period longer than is necessary to fulfill the purpose for which it is used.

3 使用 Use

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

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

4 保安措施 Security

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

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

5 透明度 Openness

資料使用者須公開其處理個人資料的政策和行事方式，交代其持有的個人資料類別和用途。

A data user must make known to the public its personal data policies and practices, types of personal data it holds and how the data is used.

6 查閱及更正 Data Access & Correction

資料當事人有權要求查閱其個人資料；若發現有關個人資料不準確，有權要求更正。

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

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

PCPD HK

PCPD.org.hk

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

"Notice" and "Consent" under PDPO

- **Collection** of Data
  - Consent not a pre-requisite
  - DPP1(3) - Focus on providing **notification** on or before data collection: -
    - **Purposes** for which data is to be used; and
    - Classes of **potential transferees** of data

"Notice" and "Consent" under PDPO

- **Use of Data**
  - DPP3(1) - Prescribed consent if use data for new purposes (subject to exemption provisions)
    - S.2(3) - Express consent given voluntarily and not withdrawn in writing
    - No prescribed consent is implied from data subject's conduct, silence or omission
    - Must be informed consent
  - DPP3(2) - Prescribed consent to be given by relevant person on behalf of vulnerable data subjects

Positions of OECD Privacy Guidelines

- **Collection Limitation** Principle (Para 7, Part 2)
  - Personal data should be collected by lawful and fair means, and **where appropriate**, with the **knowledge or consent** of data subject

- **Purpose Specification** Principle (Para 9, Part 2)
  - Purposes for which personal data are collected should be specified not later than at the time of collection and on each occasion of change of purpose

Positions of OECD Privacy Guidelines

- **Use Limitation Principle (Para 10, Part 2)**
  - Personal data should not be used or disclosed for purposes other than collection purpose, except (i) with consent of data subject; or (ii) by authority of law

Implementation of GDPR

More stringent requirements on "Notice" and "Consent" under GDPR to ensure legal certainty among EU member states

- **Effective from 25 May 2018**
- **Extra-territorial application**
- **Even no establishment in the EU, applies to data users if offer goods and services to EU citizens or monitor behaviours of individuals in the EU**

"Notice" Requirements under GDPR

- Article 13(1) – Information to be provided where personal data collected from data subjects
  - ➢ Identity and contact details of controller
  - ➢ Contact details of data protection officer
  - ➢ Purposes of processing and the legal basis
  - ➢ Legitimate interests pursued by controller
  - ➢ Recipients of personal data

"Notice" Requirements under GDPR

- Article 13(2) – Further information to ensure fair and transparent processing
  - Data storage period and the criteria
  - Existence of access to and rectification or erasure of personal data
  - Existence of right to withdraw consent
  - Right to lodge complaint
  - Consequences of failure to provide data
  - Existence of automated decision-making and profiling

- Article 14(2) – Also inform data subject of the source from which personal data originate

"Consent" Requirements GDPR

- Definition of "Consent" under Article 4(11)
  - Agreement by a statement or a clear affirmative action
  - Must be freely given, specific, informed and unambiguous

- Examples signalling "Consent" (Recital 32)
  - Ticking a box when visiting an internet website
  - Choosing technical settings for information society services

- Examples not signalling "Consent" (Recital 32)
  - Silence
  - Pre-ticked boxes
  - Inactivity

"Consent" Requirements GDPR

- Recital 43 & Article 7(4) - Data user may not make a service conditional upon consent (bundled consent), unless processing is necessary for the service

- Article 8(1) - Parental consent required for processing of personal data of children under the age of 16 (or 13) for online activities

❖ triggers discussions on how these core values / principles can best serve data privacy protection in digital environment

"Notice"

- Too many notices; too long; too complex
- Too far-reaching; not specific or limited
- Too diverse; not standardised
- Sometimes hard to locate; sometimes totally absent
- One-sided, not to inform data subject, merely to protect data user
- Sometimes presented at moment of weakness/need for individual

"Consent"

- **Uninformed** consent (inadequate notice) undermines trust and mutual respect
- **Impossible for big data analytics** involving ubiquitous data collection
- **Over reliance** on consent would **stifle data processing** for genuine needs; data subject may develop "**consent fatigue**"

Challenges of Notice & Consent Model

- Wider use of data, online services and emergence of connected technologies surfaced the "inadequacies" of "Notice" and "Consent"
- Drifting towards "legitimate interest" ground
- Individuals have reduced control and respect in the digital age
  - ➢ Uninformed "Notice" and "Consent" lead to widespread use of data for digital marketing and profiling beyond one's expectation

Challenges of Notice & Consent Model

- **Regulators face an impossible task with limited resources**
  - **In the digital age, data may be: -**
    - **"Provided" (purchase, applications, Instagram)**
    - **"Observed" (cookies, location services, CCTV images)**
    - **"Derived" (credit ratios, average purchase per visit)**
    - **"Inferred" (credit score, behaviour predictions)**
  - **Regulators' hands are full with just the "Provided" data**

How to Address the Challenges of Notice & Consent Model

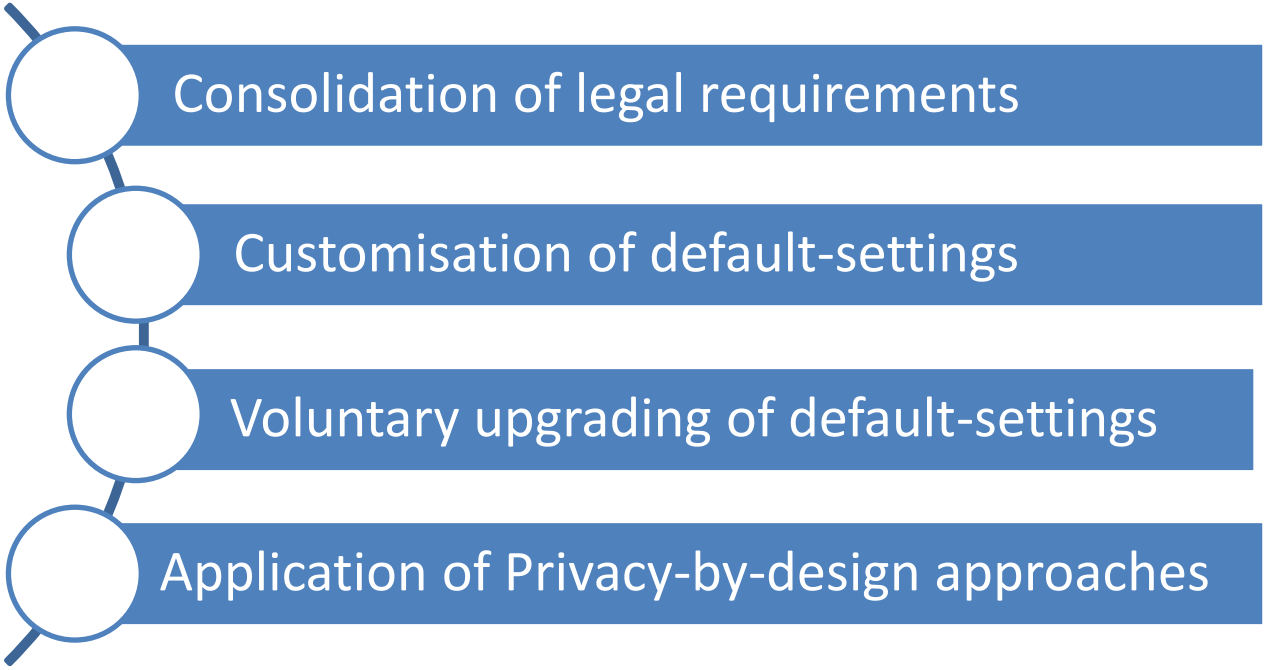
Main theme: -

- An **ethical** issue with proper data governance regime as back up
- Find ways to empower **individuals** allowing them to **regain control, responsibility and agency**
- Individuals and organisations should treat each other with **dignity, growing trust and friendship**
- Development : International research and collaboration (e.g. Privacy Bridge Projects)

How to Address the Challenges of Notice & Consent Model

- **Enhance "User Control" (meaningful; effective; trusted)**

Four measures



How to Address the Challenges of Notice & Consent Model

- Enhance "User Control" (meaningful; effective; trusted)
  - ➢ What is needed to make "user control" effective?
    - ❑ embeds privacy into architecture of system (technology & design)
    - ❑ takes into account human capabilities and constraints when devising privacy controls
    - ❑ embraces right attitudes (responsibility, openness, fairness, respect, scalability) by service providers and platforms to guarantee data protection
    - ❑ implementation of law by the authority through incentives, guidance and enforcement

How to Address the Challenges of Notice & Consent Model

- Enhance "User Control" (cont'd)
  - ➢ Example: Privacy Dashboard
    - ❑ Realistic and feasible
    - ❑ Comprehensive
    - ❑ Privacy-friendly default-setting
    - ❑ Granular controls
    - ❑ Scalable and persistent
    - ❑ Technically enforced
    - ❑ Trustworthy and fair
    - ❑ Transparent and verifiable

Example of Privacy Dashboard

How to Address the Challenges of Notice & Consent Model

- **Focus on "Security and Ethics"**
  - **Risk assessment**
    - Weighing benefits of data collection against the risks concerned without consent
    - Should cover not just data breach, but also **dignity** and **autonomy** of individuals
  - **"Do No Harm" Principle**
    - Recital 75 of GDPR identified data processing which could result in a risk to the rights and freedoms of natural persons, eg where processing may give rise to discrimination, or where personal aspects are evaluated, etc

How to Address the Challenges of Notice & Consent Model

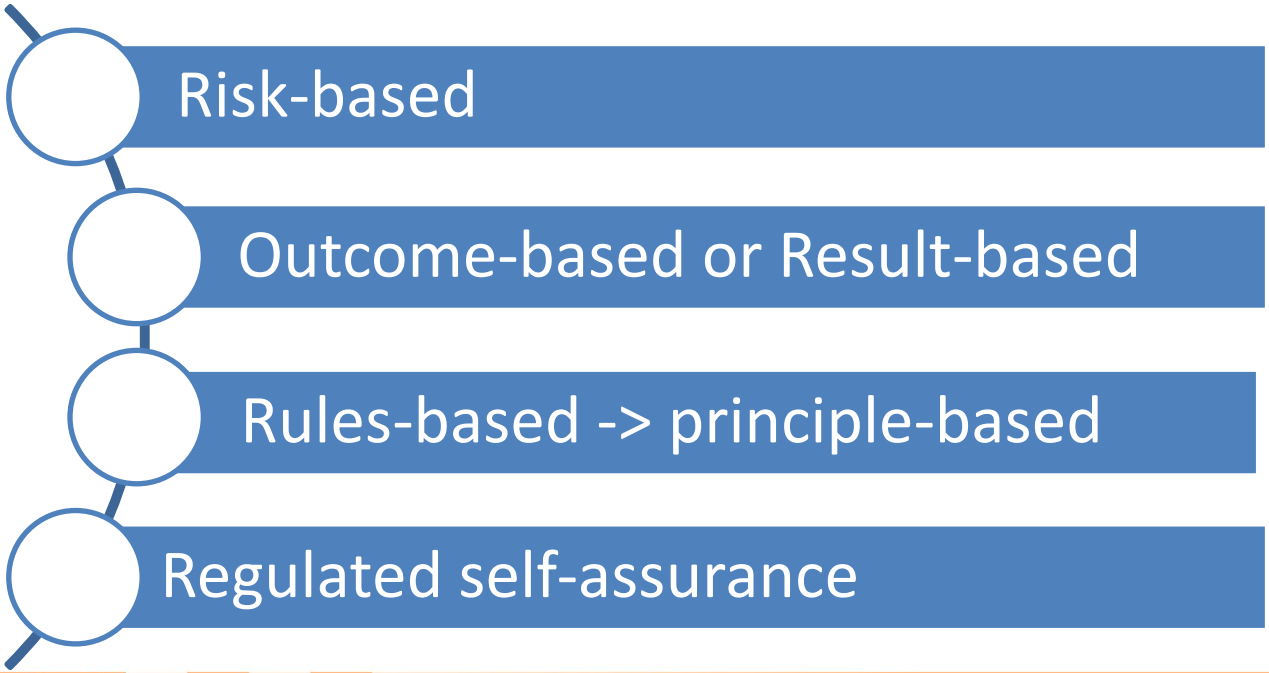
- **Promote "Accountability"**
  - ➢ **Enhance transparency in data collection and processing, especially for IoT through: -**
    - ❑ **Implementing Privacy by design**
    - ❑ **Conducting Privacy Impact Assessment**
    - ❑ **Adopting Privacy Management Tools**
  - ➢ **Redress for individuals**
    - ❑ **Contractual clauses to ensure sufficient protection and to provide for proper redress**
    - ❑ **Technology to avoid re-identification of anonymised data**
    - ❑ **Proper use of eg for genuine research**
    - ❑ **Monitoring and oversight**

How to Address the Challenges of Notice & Consent Model

- **Ensure "Fairness"**
  - ➢ **Fair assessment of proportionality**
    - ❑ **Is the processing disproportionate to an individual?**
  - ➢ **Legitimate interest**
    - ❑ **Is the processing necessary?**
  - ➢ **Higher barrier for sensitive data**
    - ❑ **How to balance social benefits and individuals' rights?**
  - ➢ **Explore the idea of pseudonymisation**
    - ❑ **Is it really pseudonymised?**

Smart Regulation in Digital Economy

Evolution in global regulation (regulatory theory and models): more flexibility



Desired Approach

Combined Stick and Carrot

- **Proportionate sanction (to give deterrent effect; dependent upon circumstances)**
- **Affecting behaviours and culture (fairness, privacy respectful, motivated voluntary compliance, etc.)**
- **Build up trusted relationship (through discussion and engagement)**

Strategies (1)

Need to set priorities: Selective to be effective; "Results-based approach"

- **Top priority: constructive engagement (engaging with accountable regulatees)**
- **Observance on need (high complaint and enquiry figures on certain issues are indicators)**
- **Guiding and supporting good practices**
- **Investigative role for deliberate, wilful or serious conduct**

Strategies (2)

Constructive engagement

- **Transparency and practical guidance**
- **Maximising consultation and participation (engaging with accountable regulatees and presented DPAs with suggestions for consideration from regulatees' perspective)**
- **Give incentives for good faith compliance**
- **Creating space for responsible innovation**

Regulatee's Cooperation

Organisations have self-interest to behave well

Aspects for consideration:-

- **Accountability and Governance (Privacy Management Programme: A Best Practice Guide)**
- **Cooperation with DPAs and building up a privacy respectful culture and trust (more effective than years of litigation)**
- **How to implement transparency? (apart from education and promotion, build a system that works for people, make good use of privacy management tools, e.g. Privacy-by-Design, Privacy Impact Assessment and Compliance Audit, etc.)**

Important

The contents herein are for general reference only. It does not provide an exhaustive guide to the application of the Personal Data (Privacy) Ordinance ("the Ordinance"). For a complete and definitive statement of law, direct reference should be made to the Ordinance itself.


個人資料 由你掌握
注意！這是我的個人資料私隱
注意
現可以優惠價訂講!
定價：HK$128 / HK$110
（優惠期至2017年12月31日）
Special Offer
Personal Data (Privacy) Law in Hong Kong
A Practical Guide on Compliance
20% discount
until 31 December 2017
List price: HK$598
Now: HK $478


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

Contact Us

- Hotline - 2827 2827
- Fax - 2877 7026
- Website - www.pcpd.org.hk
- E-mail - enquiry@pcpd.org.hk
- Address - 12/F, Sunlight Tower, 248 Queen's Road East, Wanchai, HK