Influence of the EU GDPR 2018 on Hong Kong’s Data Protection Landscape

Fanny Wong
Deputy Privacy Commissioner for Personal Data
Office of the Privacy Commissioner for Personal Data, Hong Kong
Presentation Outline

- Overview of Hong Kong’s data protection landscape
- Major Differences between EU’s GDPR and Hong Kong’s PDPO
- Influences of GDPR
  - Regulators
    - Legislative changes
    - Education and promotion
  - Businesses’ Response to New Restrictions and Sanctions
    - Under the local law
    - Under GDPR
  - Individuals’ New Rights
    - Under the local law
    - Under GDPR
The Personal Data Protection Landscape in Asia

- India - 2011
- Nepal - 2007
- Thailand - 1997
- Vietnam - 2010
- Malaysia - 2010
- Singapore - 2012
- Indonesia - 2016
- Japan - 2003
- S. Korea - 2011
- Taiwan - 2010
- Hong Kong - 1995
- Macau - 2005
- Philippines - 2012
- Nepal - 2007
- Thailand - 1997
- Vietnam - 2010
- Malaysia - 2010
- Singapore - 2012
- Indonesia - 2016
- Japan - 2003
- S. Korea - 2011
- Taiwan - 2010
- Hong Kong - 1995
- Macau - 2005
- Philippines - 2012
Hong Kong’s Data Protection History

- OECD Privacy Guidelines 1980
- PDPO 1995
- EC’s Data Protection Directive 1995
- PDPO Major Amendments 2012
- EU GDPR 2018
- Now

PDPO

Now
EU General Data Protection Regulation (GDPR)

- Enacted in May 2016
- Will be implemented on 25 May 2018
- Will replace 1995 EC Data Protection Directive (95/46/EC)
- Harmonises data protection laws across EU member states
Background

- Keep abreast with overseas’ privacy law developments
- Assess GDPR’s impact on businesses (in particular multi-national organisations) and to issue guidelines to data users, if necessary
- Harmonise legal framework to facilitate free flow of information and commercial activities
## PDPO – GDPR Comparative Study

### Major differences identified by PCPD

<table>
<thead>
<tr>
<th>1. Extra-Territorial Application</th>
<th>2. Accountability</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>3. Mandatory Breach Notification</strong></td>
<td>4. Sensitive Personal Data</td>
</tr>
<tr>
<td>5. Consent</td>
<td><strong>6. Data Processors’ Obligations</strong></td>
</tr>
<tr>
<td><strong>9. Sanctions</strong></td>
<td></td>
</tr>
</tbody>
</table>
Influences of GDPR

GDPR’s Influence on Regulator

- Mandatory Breach Notification?
- Sanctions?
- Data Processors’ Obligations?

All Hong Kong data users would be affected by changes implemented in Hong Kong
Mandatory Breach Notification

**GDPR**
- Notify data protection authority without undue delay
- Notify affected data subjects for high-risk breaches

**PDPO**
- No mandatory requirement to notify
- Voluntary breach notification

[PCPD.org.hk]
Sanctions

**GDPR**

- Administrative fine up to €20 million, or 4% of the total worldwide annual turnover of preceding financial year, whichever is higher, for serious breaches of the GDPR

**PDPO**

- Serve enforcement notices on organisations in breach of DPPs
- Breach of enforcement notice is a criminal offence
- Other offence provisions concern mainly direct marketing activities
Data Processors’ Obligations

GDPR

- New obligations, such as maintaining records of processing, ensuring security of processing, reporting data breaches, designating Data Protection Officers, etc. are imposed on data processors.

PDPO

- Data processors are not directly regulated.
- Data users are required to adopt contractual or other means to ensure data processors’ compliance in certain aspects.
Influences of GDPR

GDPR’s Influence on Businesses

- Extra-Territorial Application
- Sanctions
- Accountability

e.g.
Extra-Territorial Application

GDPR

• Apply to a controller or processor established outside EU, so long as (a) the offering of goods or services; or (b) the monitoring of the behaviour are targeted at EU individuals.

PDPO

• Apply to data users which control the processing of personal data in or from Hong Kong
• No explicit provision imposing obligations on data users outside Hong Kong, nor expressly confers rights upon data subjects not present in Hong Kong
Sanctions

GDPR

- Administrative fine up to €20 million, or 4% of the total worldwide annual turnover of preceding financial year, whichever is higher, for serious breaches of the GDPR

PDPO

- Serve enforcement notices on organisations in breach of DPPs
- Breach of enforcement notice is a criminal offence
- Other offence provisions concern mainly direct marketing activities
Accountability

GDPR

• Expressly states the accountability principle
• Specific measures to implement accountability (e.g. appointment of data protection officer, DPIA, privacy by design)
• Designate data protection officer if: (a) public body conducts data processing; (b) core activities involve large-scale data subjects monitoring; or (c) core activities involve large-scale sensitive data processing

PDPO

• Not explicitly state the accountability principle
• PMP to encourage organisations to shift from compliance to accountability. Leaflet on “Privacy Impact Assessment”.
Influences of GDPR

New Rights Given to Individuals under GDPR

Consent

Sensitive Personal Data

Other New and Enhanced Rights
Consent

GDPR

- freely given, specific, informed and unambiguous agreement to processing by a statement or a clear affirmative action

PDPO

- Data collection – not prerequisite (focus on providing notice by data users)
- Data use – prescribed consent if use data for new purposes
  → express consent given voluntarily and not withdrawn in writing
Sensitive Personal Data

GDPR

- Expanded the categories to include genetic data, biometric data, sexual orientation
- Processing of sensitive personal data is allowed only under specified circumstances

PDPO

- No distinction between sensitive and non-sensitive personal data
Other New and Enhanced Rights

### GDPR

- Right to erasure (or ‘right to be forgotten’)
- Right to data portability
- Right to object to processing (including profiling), etc.

### PDPO

- No general right to erasure, but has requirement on retention period
- No right to data portability
- No general right to object, but may opt out from direct marketing
Conclusion

• The EU’s GDPR is envisaged to bring significant impact on non-EU businesses due to its extra-territoriality, especially multinational companies (note: sanctions)

• Businesses should ensure that they are GDPR-ready

• Businesses should start to review their internal privacy policies and controls and identify gaps in GDPR compliance
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

Copyright

This PowerPoint is licensed under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. In essence, you are free to share and adapt this PowerPoint, as long as you attribute the work to the Office of the Privacy Commissioner for Personal Data, Hong Kong. For details, please visit creativecommons.org/licenses/by/4.0.
Thank you

Danke
terima kasih
gracias
mercì

спасибо
dziękuję
obrigado

ngiyabonga
teşekkür ederim
mochchakkeram
gó raibh maith agat

bedankt
hyala
unna

sukriya
kop khun krap
grazie
arigató

dank je

sagol

go tak

merci

dakujem

감사합니다

merci

tapadhl eat