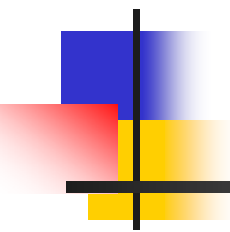


Panel on Constitutional Affairs
Meeting on 18 October



Report on Public Consultation on
Review of the Personal Data
(Privacy) Ordinance

Constitutional and Mainland Affairs Bureau
October 2010



Major proposals to be taken forward

- A total of 37 proposals to be taken forward. The major ones include:
 - a) Direct marketing and related matters
 - b) Data security
 - c) Powers of Privacy Commissioner
 - d) New offences and sanctions



Proposal (1):

Collection and use of personal data in direct marketing (1/7)

Current Provisions:

- **Data Protection Principle (“DPP”)1:** data user should take all practicable steps to ensure that the data subject is explicitly informed of the **use purpose** and the **classes of transferees**
- **DPP3:** the data subject’s **prescribed consent** is required if his/her personal data are to be used for a purpose other than the purpose for which the data were to be used at the time of collection of the data or a directly related purpose
- Violation of DPPs → issue of **enforcement notice (“EN”)**;
Non-compliance with EN → liable on conviction to **a fine at level 5 (\$50,000) and to imprisonment for 2 years**



Proposal (1):

Collection and use of personal data in direct marketing (2/7)

- **Major criticism**: some enterprises transfer customer personal data for direct marketing purposes -
 - (a) without explicitly and specifically informing customers of the purpose of the transfer and the identity of the transferees
 - (b) information in small print
 - (c) bundled consent



Proposal (1):

Collection and use of personal data in direct marketing (3/7)

- Some LegCo Members and concern groups have called for more stringent regulation
- General view is not to prohibit enterprises from using customer personal data for direct marketing purposes, but rather customers should be given an informed choice as to whether to allow data users to use their personal data for such purposes



Proposal (1):

Collection and use of personal data in direct marketing (4/7)

New requirements

If a data user intends to use the personal data collected for direct marketing purposes:

- a) Data user's Personal Information Collection Statement ("PICS") : should be reasonably specific about (i) the intended direct marketing activities; (ii) classes of transferees; and (iii) the kinds of data to be transferred;
- b) Presentation of information at (a) above : understandable and reasonably readable by general public; and
- c) Provide an option for data users to choose not to agree (e.g. by ticking a checkbox) to use or transfer of data for marketing

Non-compliance with any of the requirements in (a) to (c) → issue of an EN



Proposal (1):

Collection and use of personal data in direct marketing (5/7)

- The Privacy Commissioner for Personal Data (“PCPD”) has just issued a new guidance note on the collection and use of personal data for direct marketing
- To tie in without the entry into force of the new requirements, we propose that the PCPD should take into account the new requirements and revise the guidance note, or replace it with a Code of Practice in consultation with relevant stakeholders as appropriate to provide guidance on the new requirements
- The PCPD will also launch a publicity and public education programme to promote understanding of the new requirements by both data users and data subjects, and assist data users in complying with the new requirements



Proposal (1):

Collection and use of personal data in direct marketing (6/7)

Offences

- a) Does not comply with any of the above requirements AND subsequently uses (including transfers) the personal data for direct marketing purposes; or
- b) Complies with requirements but uses (including transfers) the personal data for a marketing activity or transfers the data to a class of transferees to which the data subject has indicated disagreement; or
- c) Uses (including transfers) the personal data for a marketing activity, transfers the data to a class of persons or transfers a kind of data not covered in the PICS

Penalty: a fine of \$500,000 and imprisonment for 3 years



Proposal (1):

Collection and use of personal data in direct marketing (7/7)

Raising penalty for misuse of personal data in direct marketing

- Under s. 34 of PDPO, a data user shall not use any personal data for the purpose of carrying out direct marketing activities if the data subject has previously requested the data user to cease to so use them

Penalty: raise from a fine at level 3 (\$10,000) to a **fine of \$500,000** and **imprisonment for 3 years**



Proposal (2): Unauthorised sale of personal data by data user (1/3)

Considerations

- There are calls for criminalising sale of personal data by data users. There are, however, views that the resulting damage does not warrant outright criminalization.
- Some consider that data users should be allowed to sell the personal data if the data subjects consent to the sale



Proposal (2): Unauthorised sale of personal data by data user (2/3)

New Requirements

- a) Data user should inform the data subject in writing of the kinds of personal data to be sold and to whom they will be sold;
- b) Presentation of information at (a) above : understandable and reasonably readable by general public; and
- c) Provide data subject with opportunity to indicate whether he/she agrees to (“opt-in”) or disagrees with (“opt-out”) the sale

Non-compliance with any of the requirements in (a) to (c)

→ issue of an EN



Proposal (2): Unauthorised sale of personal data by data user (3/3)

- It will be an offence for a data user to sell personal data to another person for a monetary or in kind gain without complying with the requirements in (a) to (c) or against the wish of the data subject
- **Penalty:** If implemented, Hong Kong will be in the forefront. We take an open stance and cited for reference in the consultation report the penalties for a broadly similar offence in the Unsolicited Electronic Messages Ordinance, i.e. a fine of \$1,000,000 and imprisonment for 5 years. We welcome public views before taking a view on the matter.



Proposal (3): Disclosure for profits or malicious purposes of personal data obtained without the data user's consent

- A new offence
- Definition of “malicious purpose”: one possible formulation is to define it as “with a view to gain for oneself or another, or with an intent to cause loss, which includes injury to feelings, to another”
- As this offence also concerns the sale of personal data, one option is to set the penalty at the same level as that for the offence concerning unauthorised sale of personal data aforementioned. To take a view after the public discussions.



Data Security (1/2)

Proposal (5):

Regulation of data processors and sub-contracting activities

- Continue to adopt indirect regulation approach and further require data users to use contractual or other means to ensure data processors' compliance with relevant PDPO requirements when contracting out the processing of personal data
- Reasons : as some data processors only provide a platform for data processing, they may not know whether the data that they are processing contain personal data or their use purpose. Adopting a direct regulation approach with increase the burden and operating costs of the industry
- Contravention → issue of an EN



Data Security (2/2)

Proposal (6): Personal data security breach notification

- The majority views supported a voluntary notification system. As notification system is still in development stage without clean or objective notification standards or common practices, if a mandatory system is adopted, data users worried how the system is going to operate and the onerous burden brought to them
- Propose voluntary system and will adjust detailed arrangements having regard to operational experience
- In June 2010, the PCPD promulgated a guidance note entitled “Data Breach Handling and the Giving of Breach Notifications”
- The Office of the PCPD will take promotional and educational initiatives to promote the adoption of a data breach notification system and assist data users to make appropriate notification



Powers of the PCPD

Proposal (7): Legal assistance to data subjects

- To confer the PCPD with the power to provide legal assistance to an aggrieved data subject who intends to institute legal proceedings against a data user to seek compensation under s. 66 of PDPO
- The legal assistance may include: giving legal advice on the sufficiency of evidence, arranging for a lawyer from the Office of the PCPD to act as the legal representative of the applicant, arranging for either a lawyer from the Office of the PCPD or an outside lawyer to represent the applicant in legal proceedings, and providing any form of assistance which the Office of the PCPD considers appropriate



New Offences and Sanctions

Proposal (18): Repeated contravention of a Data Protection Principle on same facts

- Making it an offence, as against the existing arrangement of issuing an EN again. Penalty at a fine at level 5 (\$50,000) and imprisonment for 2 years

Proposal (19): Repeated non-compliance with Enforcement Notice

- Raise the penalty, from the existing fine at level 5 (\$50,000) to a fine at level 6 (\$100,000), and maintain the term of imprisonment at the existing level of two years



Proposals not to be taken forward (1/4)

- Having regard to public views received, 7 proposals, as well as proposals indicated not to be pursued in Annex 2 to consultation document, are not to be taken forward. The major ones include :
 - a) Sensitive personal data
 - b) Granting criminal investigation and prosecution power to the PCPD
 - c) Empowering the PCPD to award compensation to aggrieved data subjects
 - d) Empowering the PCPD to impose monetary penalty on serious contravention of DPPs



Proposals not to be taken forward (2/4)

Proposal (38): Sensitive personal data

- Wide impact on community
- No mainstream views on coverage of sensitive personal data and regulation mode
- Strong objections from the IT sector to classify biometric data as sensitive personal data
- We propose that:
 - (a) the Office of the PCPD should step up promotion and education and, where necessary, issue codes of practice or guidelines on sensitive personal data
 - (b) the PCPD should continue to discuss with the information technology sector possible measures to enhance the protection of biometric data



Proposals not to be taken forward (3/4)

Proposal (39): Granting criminal investigation and prosecution power to the PCPD

- Not to pursue the proposal to confer the PCPD with the power to carry out criminal investigations and prosecutions. Should continue having separate organisations to handle investigations and prosecutions to ensure checks and balances

Proposal (40): Empowering the PCPD to award compensation to aggrieved data subjects

- Not to pursue the proposal to empower the PCPD to determine the amount of compensation to a data subject who suffers damage by reason of a contravention of a requirement under the PDPO by a data user. Inappropriate to confer enforcement power and power to grant compensation to the same organisation



Proposals not to be taken forward (4/4)

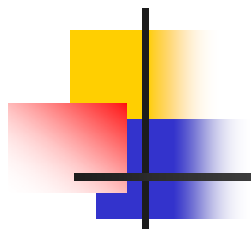
Proposal (42): Empowering the PCPD to impose monetary penalty on serious contravention of DPPs

- Not to pursue the proposal to confer the PCPD with the power to impose monetary penalty on data users for serious contravention of DPPs
- Public views considered it inappropriate to put the enforcement power and power to impose penalty in the same organisation
- We consider it more appropriate to make serious contravention a criminal offence



Further Public Discussions

- Will invite the public to further discuss the legislative proposals, for a period of more than two months, until the end of December
- We welcome public views on the specific arrangements and details of the proposals to be taken forward. In addition, we shall arrange to meet with relevant organisations and stakeholders for in-depth discussions on the details of the proposals to be taken forward



- Thank you -