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

專員用箋 From the desk of the Commissioner

Your Ref: CB2/PL/CA
Our Ref: PCPD(O)125/115/25 pt.6

**(By Email)**

28 January 2014

Hon TAM Yiu-chung, GBS, JP
Chairman of Panel on Constitutional Affairs
Legislative Council
Legislative Council Complex
1 Legislative Council Road
Central, Hong Kong

Dear Mr Tam

**Report on the Work**
**of the Office of the Privacy Commissioner for Personal Data (PCPD) in 2013**

I attended the Panel Meeting on 21 January 2013 to update Panel members on the work of the PCPD in 2012.

For the Panel's information, I attach a report on PCPD's accomplishments in 2013. If it is considered necessary by the Panel, I am prepared to attend the meeting of the Panel to brief members on the paper and exchange views with them on related issues.

Yours sincerely,

(Allan CHIANG)
Privacy Commissioner for Personal Data

Encl.

c.c. Secretary for Constitutional and Mainland Affairs
(Attn: Mr Gordon LEUNG, JP)

香港灣仔皇后大道東248號12樓 12/F, 248 Queen's Road East,
Wanchai, Hong Kong 電話 Tel (852) 2877 7168 傳真 Fax (852) 2877 7026
電郵 Email allan.chiang@pcpd.org.hk 網址 Website www.pcpd.org.hk

**Legislative Council Panel on Constitutional Affairs**

**Report on the Work**
**of the Office of the Privacy Commissioner for Personal Data in 2013**

Members were briefed at the meeting of the Legislative Council Panel on Constitutional Affairs on 21 January 2013 by the Privacy Commissioner for Personal Data ("the Commissioner") on the accomplishments of his office ("PCPD") in 2012. This paper serves to update Members of PCPD's work in 2013.

## Enquiries and Response to Consultations

2. In 2013, PCPD received a total of 24,161 enquiry cases, representing a record high and an increase of 27% compared with 2012. They are mainly concerned with the use of personal data in direct marketing (55%), employment (10%), data access requests (8%), collection of Hong Kong identity card numbers or copies (5%), and workplace surveillance (2%).

3. In particular, 13,203 enquiries (55% of the total) are related to the new provisions of the Personal Data (Privacy) (Amendment) Ordinance 2012 (the "Amendment Ordinance") governing the use of personal data in direct marketing. Most of them were made in April and May 2013.

4. During the year, PCPD provided detailed comments in response to consultations from various government bureaux and departments covering a wide range of subjects, and made submissions on various proposed legislative and administrative measures that have an impact on personal data privacy. Details are set out in **Annex A**.

## Complaints

5. In 2013, the PCPD received a total of 1,792 complaints, which represented a record high and an increase of 48% compared with 2012. The PCPD was able to handle this huge influx of complaints by streamlining working procedures and enhancing staff productivity.

6. Of these complaints, 78% were made against the private sector (1,404 cases), 13% against the public sector/government departments (227 cases) and 9% against individuals (161 cases).

7. Among the private sector organisations, the sector which received the most complaints was the financial sector (356 cases), followed by telecommunications (153 cases) and property management (125 cases).

8. As regards the nature of the complaints, 38% of the 1,792 complaints received concerned the use of personal data without the consent of data subjects (673 cases), 36% were about the purpose and manner of data collection (643 cases), 9% were related to data security (169 cases) and 9% were about data access/correction requests (161 cases).

9. A substantial number (538 cases) of the complaints were related to the implementation of the new provisions governing the use of personal data in direct marketing. Specifically, they were responses to the sending of a massive amount of customer notifications in late March 2013 and early April 2013 by many organisations concerning the use of personal data for direct marketing. The notifications were sent for various reasons such as:-

(a) to ensure the fulfilment of one of the pre-requisite requirements of the grandfathering arrangement, namely, that the customers had to be explicitly informed, in a easily understandable and readable manner, of their intended use of their personal data for direct marketing;

(b) to include as many classes of products and services as possible for grandfathering coverage when in fact only those classes for which a direct marketing approach has actually been made previously could be covered; and

(c) to carry out data cleansing by reminding customers of their right to opt out from direct marketing approaches.

10. The ensuing complaints can be categorised as follows:-

(a) the notifications erroneously created a perceived need on the part of the customers to respond promptly or else their position as regards the right to opt out from direct marketing approaches would be jeopardised;

(b) the opt-out channels stipulated by the organisations were fully engaged, not user-friendly or invalid; and

(c) some recipients queried why their personal data were held by the organisations which sent out the notifications since according to them, they had no prior dealings with the organisations.

11. Further, a total of 93 complaints (compared with 50 complaints in 2012) were related to the use of new information and communications technologies ("ICT"). Of these, 40 related to the unwanted disclosure of individuals' personal data on social networking sites and 12 concerned the receipt of unsolicited direct marketing messages through WhatsApp. These cases could not be pursued meaningfully. For the former cases, the person responsible for the data could not be traced. For the latter cases, the calls were made to randomly selected telephone numbers without the use of personal data.

**Compliance Checks and Self-initiated Investigations**

12. The year 2013 saw 61 known data breach incidents (compared with 50 incidents in 2012), affecting 90,000 individuals. The PCPD was made aware of these incidents through voluntary notifications from the data users concerned as well as reports from the media and the general public. The nature of these incidents ranged from unauthorised disclosure of personal data through hacking to inadvertent circulation of lists of personal data to unrelated third parties.

13. With a view to promoting compliance with the requirements under the Personal Data (Privacy) Ordinance ("the Ordinance"), the PCPD completed 208 compliance checks and 19 self-initiated investigations in 2013, compared with 161 such checks and 9 such investigations respectively in 2012.

14. Much work has been done in the area of ICT applications. A survey of 60 smartphone apps developed by Hong Kong entities revealed that their transparency in terms of privacy policy was generally inadequate. Only 60% of the apps provided Privacy Policy Statements and most of them did not explain what smartphone data they would access and the purposes for the access. Most of them have been advised to make improvement. Even if they did not collect the customers' personal data to which the apps had access, they were encouraged to make known their non-collection policy.

**Investigation results**

15. In 2013, the PCPD issued 32 warnings and 25 enforcement notices to organisations, compared with 27 warnings and 11 enforcement notices in 2012. The more than double increase in the number of enforcement notices issued to direct organisations to remedy contraventions was a reflection of the enhanced power of the Commissioner to exercise such enforcement power under the Amendment Ordinance.

16. The Commissioner published 6 investigation reports in 2013 (compared with 8 published reports in 2012). These reports (see details at **Annex B**) covered the privacy practices of 3 companies, one government department and one public body, and pointed out contraventions of Data Protection Principle ("DPP") 1 concerning data collection, DPP 3 concerning data use and DPP4 concerning data security.

17. The reports received widespread media coverage and entailed serious public discussion. They served to invoke the sanction and discipline of public scrutiny and discourage non-compliant behaviour on the part of the organisations concerned as well as other data users facing similar data-protection issues.

**Prosecution**

18. In 2013, the PCPD referred 20 cases to the Police for consideration of prosecution, an increase of 33% compared to 2012. As many as 14 cases were related to suspected contraventions of the new provisions governing the use of personal data in direct marketing, for example, the making of repeated telemarketing calls by organisations despite the complainants' request to opt out from such marketing approach and the failure of organisations to take specified steps before making use of individuals' personal data for direct marketing.

19. Most of the referred cases are still under Police investigation, and no conviction was recorded in 2013.

**Inspection**

20. The PCPD completed an inspection of the CCTV systems used by the MTR Corporation to monitor the public areas of its train stations and compartments. It also completed an inspection of the personal data system used by the Student Financial Assistance Agency in administering four financial assistance schemes for primary and secondary students. The inspections identified areas for improvement of personal data privacy protection and the Commissioner has made recommendations on improvement to the two organisations. Reports on the two inspections were published in April 2013 and January 2014 respectively.

**Legal Assistance Scheme**

21. The Legal Assistance Scheme commenced on 1 April 2013 under the Amendment Ordinance. Under the scheme, the PCPD may provide assistance to a person who has suffered damage by reason of a contravention under the Ordinance and intends to institute proceedings to seek compensation from the organisation at fault. After 9 months of operation, the PCPD has received 16 applications. Of these applications, one has been granted assistance; 5 were rejected and 2 had been withdrawn by the applicants.

**Data User Returns Scheme ("DURS")**

22. Part IV of the Ordinance provides for a DURS under which specified organisations are obliged to notify to the Commissioner "prescribed information" which includes the kinds of personal data they control and the purposes for which the personal data are collected, held, processed or used .

23. The PCPD issued a consultation document in July 2011 which outlined the operational framework and implementation plan of the DURS. It was envisaged that the initial phase of implementing the DURS would cover the government and public bodies as well as the banking, telecommunications and insurance sectors.

24. The PCPD gathered from the consultation exercise that while there was no dispute over the objective of DURS to promote a higher standard in the protection of personal data privacy, there was much scepticism from the consultees towards the adoption of the scheme to achieve this objective. At the same time, PCPD has learned that the European Union ("EU") data protection system, upon which the Hong Kong model is based, is undergoing reform. Among other things, the EU is considering replacing the notification requirement with new and improved systems which emphasize accountability and transparency in the collection and use of personal data, including the mandatory appointment of a data protection officer in (a) public authorities and bodies, as well as (b) private enterprises that process data of more than 5,000 persons in any consecutive 12 months.

25. In the absence of general support from the 4 sectors identified for implementing the DURS and in light of the EU developments, the PCPD will put the project on hold until the reforms in the EU have been finalised and useful lessons can be learnt from the exercise.

26. Meanwhile, to meet the high public expectation for protection of personal data privacy in the four sectors concerned, the Commissioner has advocated to these sectors to adopt a strategic shift from compliance to accountability. Individual organisations are encouraged to embrace privacy and data protection as part of corporate governance responsibilities and implement holistic and encompassing privacy management programmes ("PMP") which ensure that robust privacy policies and procedures are in place and applied throughout the organisation. At the minimum, the outcome of this proactive approach is a demonstrable capacity to comply with the Ordinance. Executed well, PMP is conducive to building trustful relationships with customers or citizens, employees, shareholders and regulators. It thus serves the same purpose as DURS and is a good interim substitute.

27. The Commissioner has secured significant buy-in from these sectors. In February 2014, he will make public a list of organisations which have pledged to implement PMP, and issue a 'Privacy Management Programme: a Best Practice Guide' for the reference by all organisations. A chart showing the building blocks of PMP is at **Annex C**.

**Regulating Cross-border Flows of Personal Data**

28. Section 33 of the Ordinance provides a stringent and comprehensive regulation of the transfer of data outside Hong Kong. It expressly prohibits all transfers of personal data 'to a place outside Hong Kong' except in specified circumstances such as:-

(a) the place is specified by the Commissioner as one which has in force a data protection law which is substantially similar to, or serves the same purpose as the Ordinance [section 33(2)(a)]; and

(b) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be handled in a manner tantamount to a contravention of a requirement under the Ordinance [section 33(2)(f)].

29. As section 33 has not been brought into force since its enactment in 1995 and the Government has no timetable for its implementation in future, the current protection for personal data transferred overseas is weak and far from comprehensive.

30. Countries worldwide are adopting a range of mechanisms to protect the personal data privacy of individuals in the context of cross-border data flows. For example, section 26(1) of Singapore's Personal Data Protection Act, which will come into force in July 2014, provides that an organisation shall not transfer any personal data to a country or territory outside Singapore except in accordance with requirements prescribed under the Act to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the Act.

31. Against this background, it is high time for the Government to have a renewed focus on section 33 of the Ordinance to ensure that the international status of Hong Kong as a financial centre and a data hub will be preserved.

32. To assist the Government in this area, the PCPD completed in 2013 a survey of 50 jurisdictions and compiled a "white list" of places which have in force a data protection law which is substantially similar to, or serves the same purpose as the Ordinance. A copy of the report has been forwarded to the Government.

**Promotion and Public Education**

33. In 2013, the PCPD continued to step up its promotion and public education efforts to promote the awareness and understanding of privacy and data protection. A total of 279 seminars were conducted (compared with 238 in 2012), with a total audience of 20,898 (compared with 16,321 in 2012). These included free introductory seminars on personal data protection, free IT seminars educating the public on the smart use of communication technologies and professional workshops for data protection practitioners.

34. A major theme of the promotion and education activities in 2013 was the new provisions under the Amendment Ordinance governing the use of personal data in direct marketing. These activities are summarised at **Annex D**.

35. Other major themes in 2013 were On-line Privacy Protection and Smart Use of Smartphones. Special efforts were focussed on the young people through the Student Ambassador Programme (with participation of 4,800 secondary school students, representing an increase of 142% over 2012) and the University Privacy Campaign (with participation of 33,299 students and staff, representing an eleven-fold increase over 2,570 participants in 2012).

36. In running its various promotion and education activities, the PCPD partnered with various trade associations and professional bodies. It also engaged the public through multi-channels including exhibition roadshow, the mass media, and for the first time in 2013, dedicated YouTube Channel, Facebook page and the PCPD's thematic websites. The PCPD website had a facelift of its landing page during the year, and it received an average of 75,912 visits per month (compared with 45,192 visits per month in 2012).

**Strategic Focus for 2014**

37. The PCPD will continue to face the privacy and data protection challenges by stepping up efforts in enforcement as well as public education. There will be a special focus on:-

(a) the privacy issues associated with the increased use of mobile apps;

(b) the need for organisations to embrace privacy and data protection as part of their corporate governance responsibilities and adopt holistic privacy management programmes; and

(c) assisting the Government in reviewing the regulatory issues concerning cross-border flows of personal data.

**Office of the Privacy Commissioner for Personal Data**
**28 January 2014**

**Annex A**

## Responses to Consultations / Vetting of Bills in 2013

PCPD vetted altogether 61 bills and regulations published in the Government Gazette. PCPD provided comments on the following in light of their personal data privacy implications and has no comments on other bills:-

(1) Companies (Directors' Report) Regulation;

(2) Merchant Shipping (Seafarers) (Amendment) Bill 2013;

(3) Inland Revenue (Amendment) Bill 2013; and

(4) Waste Disposal (Amendment) Bill 2013.

PCPD also provided comments in response to 11 proposed legislations and government administrative measures listed as follows:-

(1) Food and Health Bureau: Private Columbaria Bill – Detailed Drafting Instructions ;

(2) Financial Services and the Treasury Bureau: Public Register of "Systemically Important Participants";

(3) Financial Services and the Treasury Bureau: Insurance Companies (Amendment) Bill 2014 regarding the establishment of an independent Insurance Authority;

(4) Financial Services and the Treasury Bureau: Companies (Residential Addresses and Identification Numbers) Regulation;

(5) Development Bureau: Amendments to the Construction Workers Registration Ordinance;

(6) Food and Health Bureau: Electronic Health Record Sharing System Bill;

(7) Labour Department: Amendments to the Employment Ordinance;

(8) Transport Department: Installation of additional cameras at road junctions for taking photographs of drivers who commit red light jumping;

(9) Hong Kong Police Force: Field trial of the use of "Body Worn Video Camera" in confrontational scenarios, or when a breach of the peace has occurred or is likely to occur;

(10) Hong Kong Police Force: Field trial of the Automatic Number Plate Recognition equipment for traffic enforcement purposes; and

(11) Hong Kong Police Force: "Data Transfer Arrangement of Mentally Disordered Persons" to transfer personal data of mentally disordered persons to Hospital Authority and Social Welfare Department.

Furthermore, PCPD responded to the following public consultations from the perspective of personal data protection:-

(1) Public Consultation on Improvement of Corporate Insolvency Law Legislative Proposals; and

(2) Public Consultation on 2014 Digital 21 Strategy.

**Annex B**

**PCPD's Investigation Reports**
**January – December 2013**

1. Transfer of Personal Data Collected Unfairly from the Public by HK Preventive Association Limited to AEGON Direct Marketing Services Insurance Broker (HK) Limited for Use in Direct Marketing
(Report Number: R13–1138; Date issued: 9 April 2013)

2. Glorious Destiny Investments Limited and Brilliant United Investments Limited Publicly Disclosed Litigation and Bankruptcy Information Collected from the Public Domain to Their Customers via Smartphone Application "Do No Evil"
(Report Number: R13–9744; Date issued: 13 August 2013)

3. Hospital Authority's Breach of Data Security in Connection with Disposal of Patient Records
(Report Number: R13–6740; Date issued: 24 October 2013)

4. The Hong Kong Police Force Leaked Internal Documents Containing Personal Data via Foxy
(Report Number: R13–15218; Date issued: 24 October 2013)

5. Hong Kong Police Force's Repeated Loss of Documents Containing Personal Data
(Report Number: R13–0407; Date issued: 24 October 2013)

6. Collection of Excessive Personal Data from Membership Applicants by J.V. Fitness Limited (trading as California Fitness)
(Report Number: R13–12828; Date issued: 5 December 2013)

# Privacy Management Programme – At A Glance

Annex C

## *Part A*
## *Baseline Fundamentals*

### Organisational Commitment

| Buy-in from the Top | Data Protection Officer/Office | Reporting |
|---|---|---|
| • Top management support is key to a successful **privacy management programme** and essential for privacy-respectful culture | • Role exists and is involved where appropriate in the organisation's decision-making process<br>• Role and responsibilities for monitoring compliance of the Personal Data (Privacy) Ordinance are clearly identified and communicated throughout the organisation<br>• Responsible for the development and implementation of the programme controls and their ongoing assessment and revision<br>• Policy and procedures are in place to incorporate personal data protection into every major function involving the use of personal data | • Reporting mechanisms need to be established, and they need to be reflected in the organisation's programme controls |

### Programme Controls
**The following programme controls are in place:**

| Personal Data Inventory | Policies | Risk Assessment Tools |
|---|---|---|
| • The organisation is able to identify the personal data in its custody or control<br>• The organisation is able to identify the reasons for the collection, use and disclosure of the personal data | Covering:<br>• Collection of personal data<br>• Accuracy and retention of personal data<br>• Use of personal data including the requirements of consent<br>• Security of personal data<br>• Transparency of organisations' personal data policies and practices<br>• Access to and correction of personal data | Training & Education Requirements<br>Breach Handling<br>Data Processor Management<br>Communication |

## *Part B*
## *Ongoing Assessment and Revision*

### Oversight & Review Plan

- Develop an oversight and review plan

  Data Protection Officer or Data Protection Office should develop an oversight and review plan on a periodic basis that sets out how the effectiveness of the organisation's programme controls will be monitored and assessed.

### Assess & Revise Programme Controls Where Necessary

- Update personal data inventory
- Revise policies
- Treat risk assessment tools as evergreen
- Update training and education
- Adapt breach and incident response protocols
- Fine-tune data processor management
- Improve communication

**Annex D**

**Promotion and Public Education Activities for Introducing the New Provisions Governing the Use of Personal Data in Direct Marketing under the Personal Data (Privacy) (Amendment) Ordinance 2012 (the "Amendment Ordinance")**

<table>
<tr><th>Target Audience</th><th>Activities</th></tr>
<tr><td rowspan="4">Data users involved in the collection and use of personal data for direct marketing activities</td><td>A media briefing was held on 15 January 2013, with 30 media attended. 10 feature articles were published in the print media.<br>A media statement was issued on 28 March 2013 to remind data users of the implementation of New Direct Marketing Regulatory Regime effective from 1 April 2013.</td></tr>
<tr><td>New Guidance on Direct Marketing was issued on 15 January 2013 (available both in print and on PCPD's website).</td></tr>
<tr><td>Advertisements were placed in professional publications/newsletters of the Hong Kong General Chamber of Commerce, the Hong Kong Retail Management Association, and the Hong Kong Institute of Chartered Secretaries (March/April 2013).</td></tr>
<tr><td>36 professional workshops on Direct Marketing were held in 2013. Among these, 12 were held before the new direct marketing regulatory regime took effect on 1 April 2013. Two Executive Workshops on "Direct Marketing Activities – Best Practices and Guidance on the New Law" were delivered by external legal professionals in June and December 2013.</td></tr>
<tr><td>The enhanced regulations on Direct Marketing were introduced in the talks delivered to:
<table>
<tr><th>Date</th><th>Partner</th><th>Attendance</th></tr>
<tr><td>22 January 2013</td><td>Data Protection Officers' Club</td><td>115</td></tr>
<tr><td>6 February 2013</td><td>Hong Kong Investment Funds Association</td><td>100</td></tr>
<tr><td>15 March 2013</td><td>Hong Kong Retail Management Association</td><td>100</td></tr>
<tr><td>20 March 2013</td><td rowspan="2">Hong Kong Trade Development Council and Trade and Industry Department</td><td>150</td></tr>
<tr><td>24 April 2013</td><td>200</td></tr>
<tr><td>22 March 2013</td><td>The American Chamber of Commerce in Hong Kong</td><td>80</td></tr>
<tr><td>27 March 2013</td><td>Hong Kong Council of Social Service and NGOs</td><td>290</td></tr>
<tr><td>6 May 2013</td><td>Hong Kong Productivity Council and SMEs</td><td>140</td></tr>
<tr><td>25 June 2013</td><td>Hong Kong Retail Management Association</td><td>150</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>16 July 2013</td><td>Hong Kong General Chamber of Commerce</td><td>90</td></tr>
<tr><td>12 August 2013</td><td>Hong Kong Information Technology Federation and the Hong Kong Association of Interactive Marketing (In conjunction with Legislative Councillor (IT) Hon Charles Mok)</td><td>38</td></tr>
<tr><td>15 August 2013</td><td>Chinese Manufacturers' Association of Hong Kong</td><td>52</td></tr>
<tr><td>27 September 2013</td><td>Democratic Party</td><td>30</td></tr>
<tr><td>2 October 2013</td><td>International Business Committee</td><td>36</td></tr>
</table>
<br>A short video on Direct Marketing was uploaded onto the PCPD website in October 2012. (as of 31 December 2013: 5,858 views)</td></tr>
<tr><td>Data subjects</td><td>The Commissioner and his senior staff gave interviews/contributed articles on the subject and extensive coverage has been generated in the mass media:<br>
• Metropolis Daily (16 October 2012)<br>
• ATV News (31 December 2012)<br>
• Hong Kong Trader (20 March 2013)<br>
• Ming Pao, Apple Daily, Hong Kong Economic Times (21 March 2013)<br>
• Cable TV, RTHK Radio "Talkabout" and "Open Line Open View" (27 March 2013)<br>
• TVB News (28 March 2013)<br>
• TVB "Pleasure & Leisure" (1 April 2013)<br>
• Commercial Radio "The Tipping Point" (4 April 2013)<br>
• NOW TV "News Magazine" (10 April 2013)<br>
• RTHK "Talkabout" (10 April 2013)<br>
• TVB "On the Record" (13 April 2013)<br>
• TVB "Scoop" (14 April 2013)<br>
• TVB Pearl Report (29 April 2013)<br>
• Journal of the American Chamber of Commerce (April 2013)<br>
• 明光社通訊 (13 May 2013)<br>
• Hong Kong Economic Times (26 June 2013)<br>
• Estate Agents Authority Newsletter (June 2013)<br>
• Hong Kong Retail Management Association Newsletter (Spring Issue 2013)</td></tr>
</table>

| | |
|---|---|
| | An information leaflet on “Exercising Your Right of Consent to and Opt-out from Direct Marketing Activities under the Personal Data (Privacy) Ordinance” was issued on 15 January 2013. |
| | The contents of seminars for the public/organisations (held approximately three times per month) have been updated to cover the new regulatory requirements since January 2013. |
| | An API was released by the Constitutional and Mainland Affairs Bureau for broadcasting on TV and Radio from 21 March to 20 September 2013. |
| | An infographic was published in two Chinese newspapers, Apple Daily and Oriental Daily, on 24 April 2013 and two weekly magazines, East Week and Next Magazine, in the first week of May 2013, to illustrate how to apply the new rules on direct marketing to protect personal data. Both English and Chinese versions are available on PCPD’s website. |