Legislative Council Panel on Information Technology and Broadcasting Meeting on 12 July 2010

Agenda Item III – Information security

PURPOSE

This paper informs Members of the Panel of the actions taken / being taken by the Office of the Privacy Commissioner for Personal Data ("**PCPD**") from 1 July 2009 to 30 June 2010 with respect to the data breach incidents involving Government bureaux / departments that have been brought to the attention of PCPD.

SCOPE OF WORK

2. Section 8 of the Personal Data (Privacy) Ordinance ("**the Ordinance**") sets out the functions and powers of the Privacy Commissioner ("**the Commissioner**"), which include promotion / education in relation to protection of personal data privacy, checking compliance with the requirements of the Ordinance, and investigation in respect of complaints received or where a suspected breach is brought to the Commissioner's attention.

PROMOTION AND EDUCATION

3. Raising awareness of personal data privacy among the employees working at Government bureaux / departments continues to be a key priority for PCPD. During the reporting period, the Commissioner and his officers gave talks to over 1,000 employees from various Government bureaux / departments, including Social Welfare Department, Correctional Services Department, Housing Department, Judiciary, Education Bureau, Civil Service Bureau, Labour Department, Student Financial Assistance Agency, Government Logistics Department, Land Registry and Leisure and Cultural Services Department.

COMPLIANCE CHECKS

4. Taking an active role in carrying out compliance actions is more important than conducting investigations in response to a complaint, since the former option is effective in preventing non-compliance in advance, especially when it comes to handling massive or sensitive personal data. A compliance check will commence in response to information from a news report, a breach notification or an enquiry / referral case in which a practice appears to be inconsistent with the requirements of the Ordinance is identified.

5. During the reporting period, PCPD conducted a total of 21 compliance checks in relation to data breach incidents concerning 11 Government bureaux / departments, including Education Bureau, Food & Environmental Hygiene Department, Fire Services Department, Hongkong Post, Home Affairs Department, Hong Kong Police Force, Independent Commission Against Corruption, Innovation and Technology Commission, Leisure and Cultural Services Department, Social Welfare Department and University Grants Committee Secretariat. Out of the 21 cases, 15 cases were notified to the Commissioner by relevant Government bureaux / departments, while the remaining 6 cases were brought to the attention of PCPD through media reports. For more details, please see **Annex** to this paper.

INVESTIGATION

6. The Commissioner is empowered to investigate suspected breaches of the Ordinance either in response to a complaint or on his own initiative. Upon receipt of a complaint, it is the policy of the Commissioner in the first instance to seek, where practicable, to mediate the dispute with a view to resolving the matters informally without recourse to his formal powers of investigation.

7. Of the 1,071 complaints received during the reporting period, 9.8% (105) were complaints against Government bureaux / departments. Most such cases were settled through mediation. In other cases, where the circumstances warranted the use of the Commissioner’s powers, formal investigations were instigated.

8. Upon completion of a formal investigation, if the Commissioner considers that the data user concerned is breaching or has breached the requirements of the Ordinance, and the breach is likely to sustain or recur, the Commissioner may serve an enforcement notice on the data user directing it to take remedial measures.

9. During the reporting period, the Commissioner completed a total of 10 investigation cases in relation to Government bureaux / departments. 1 case was found unsubstantiated after investigation. The remaining 9 cases involved findings of contravention of the Ordinance and enforcement notices were issued in 7 contravention cases.

10. One of the enforcement notices was issued to a government department for its violation of the data security principle. In that case (which was initiated by a complaint), classified Government documents containing personal data were found circulating on the Internet through the use of a peer-to-peer file sharing application. That government department readily accepted the Commissioner's directions and complied with the terms of the enforcement notice in a cooperative manner.

11. The enforcement notices issued in the 6 other contravention cases were unrelated to data security issues. They were investigations about act or practice of data collection (2 cases) and the handling of data access request (4 cases).

12. As at 30 June 2010, there were 3 ongoing investigations into suspected breaches of the Ordinance by Government bureaux / departments.

13. The complaint / investigation cases mentioned in paragraphs 9 to 12 above are subject to the secrecy provisions of section 46 of the Ordinance and have not been included in the Annex.

PRIVACY COMPLIANCE AUDIT

14. The Government has been issuing smart identity cards to replace the old identity cards since 2003. To ensure that all personal data held by the Immigration Department ("**ImmD**") are handled in accordance with the

provisions of the Ordinance, the Government undertook to the Legislative Council to draw up a code of practice in consultation with the Commissioner setting out the rules on the collection, use of and access to smart identity card data, and to commission the Commissioner to conduct a Privacy Compliance Audit ("**PCA**") on the Smart Identity Card System.

15. The PCA aimed at assessing ImmD's level of compliance with the requirements of the Ordinance, identifying potential weaknesses in ImmD's data protection system, and providing recommendations for a review of ImmD's data protection system.

16. The PCPD commenced the PCA in June 2009. During the course of the PCA, the Commissioner's officers examined thousands of pages of ImmD documents, visited 19 ImmD offices / control points, interviewed 330 smart identity card applicants, and obtained information from 65 ImmD officers ranking from Assistant Director to Immigration Assistant. In addition, an on-site questionnaire survey targeted at serving ImmD employees was conducted.

17. The PCA was substantially completed in February 2010. On 31 March 2010, the Commissioner sent a draft PCA report to the Director of Immigration for his response. The Commissioner will appropriately incorporate into the final PCA report the responses he may receive. Areas requiring improvements, if any, will be factored into the proposed code of practice which will then be formalized and approved by the Commissioner in accordance with section 12 of the Ordinance. The latest meeting / discussion with the Immigration Department took place on 25 June 2010. It is expected that further meetings / discussion will be held, and the report should become available before the end of the year.

DATA BREACH NOTIFICATION

18. The Government has instituted a notification mechanism to require bureaux and departments to notify the Commissioner and affected individuals in the event of electronic data leakage. On 21 June 2010, the Commissioner published a new Guidance Note, titled *"Data Breach Handling and the Giving of Breach Notifications"* to encourage the adoption by data users of systematic

management plan to handle data breach incidents. This guidance note aims to assist data users in handling data breaches and to mitigate the loss and damage that may be caused to the data subjects concerned.

19. The Commissioner has also prepared a template for data users to use when notification to the Commissioner is called for. A copy of the Guidance Note and the template may be downloaded from the website of PCPD.

WAY FORWARD

20. In order to protect personal data privacy of individuals, a data user in this digital age should take and continue to take practical privacy protective measures from the design stage of new products or services to ensure that the personal data privacy risks are properly managed. The adoption of the Privacy-by-Design approach where privacy related impacts are assessed and addressed as an integral part from the design stage, and not as an after-thought is encouraged.

21. The Commissioner shall continue the efforts to promote compliance with the requirements of the Ordinance through education, compliance checks and enforcement actions. The Commissioner also hopes that the Government will proceed expeditiously with the legislative amendment proposed in the public consultation in 2009 so as to provide Hong Kong with an updated piece of privacy legislation that adequately protects personal data privacy.

Office of the Privacy Commissioner for Personal Data
July 2010

Annex

Legislative Council Panel on Information Technology and Broadcasting - Meeting on 12 July 2010

No.	Summary of the incident	Affected data subjects	Informed affected data subjects	Informed Privacy Commissioner	Actions taken / being taken by PCPD
Education Bureau (EDB)					
Case 1	In June 2010, EDB reported a suspected case of unauthorized access of computer, of which personal data of complainants and staff stored therein had been deleted.	20	No	Yes	PCPD has commenced an inquiry and EDB is required to furnish more information.
Food & Environmental Hygiene Department (FEHD)					
Case 2	In March 2010, FEHD reported the loss of "Daily Convict Result Information Checklists" containing convicted hawkers' personal data and staffs' salary statements.	37	Yes	Yes	PCPD conducted an inquiry. PCPD is examining further information submitted by FEHD.
Fire Services Department (FSD)					
Case 3	In July 2009, FSD reported the loss of ambulance journey record containing personal data.	8	Yes	Yes	PCPD conducted an inquiry and was satisfied with the remedial actions taken by FSD. Case closed.

Legislative Council Panel on Information Technology and Broadcasting - Meeting on 12 July 2010

No.	Summary of the incident	Affected data subjects	Informed affected data subjects	Informed Privacy Commissioner	Actions taken / being taken by PCPD
Home Affairs Department (HAD)					
Case 4	In June 2010, HAD reported the loss of village representative election voter registration forms containing personal data.	60	Yes	Yes	PCPD has commenced an inquiry and HAD is required to furnish more information.
Hong Kong Police Force (Police)					
Case 5	In July 2009, a local newspaper reported that some statement taking video tapes of Police were sent to a recycle company.	Unknown	Unknown	No	Inquiry revealed that there was no prima facie evidence against the Police. Case closed.
Case 6	In September 2009, a local newspaper reported that some Police reports and statement containing personal data had been found in a public refuse collection point in Cheung Sha Wan.	2	Yes	Yes	PCPD conducted an inquiry and was satisfied with the remedial actions taken by the Police. Case closed.
Case 7	In December 2009, a local newspaper reported that police files were accessible on the Internet by “Foxy” users.	18	15	No	PCPD conducted an inquiry and was satisfied with the remedial actions taken by the Police. Case closed.

No.	Summary of the incident	Affected data subjects	Informed affected data subjects	Informed Privacy Commissioner	Actions taken / being taken by PCPD
Case 8	In December 2009, a local newspaper reported that some more police files were accessible on the Internet by "Foxy" users.	131	96	Yes	PCPD conducted an inquiry and was satisfied with the remedial actions taken by the Police. Case closed.
Case 9	In January 2010, the Police reported that they had lost a handwriting notebook containing personal data in relation to a traffic accident case.	2	Yes	Yes	PCPD conducted an inquiry. PCPD is examining further information submitted by the Police.
Case 10	In May 2010, the Police reported that a police officer had left two case files containing personal data in a taxi.	7	Yes	Yes	PCPD conducted an inquiry. PCPD is examining further information submitted by the Police.
Case 11	In May 2010, the Auxiliary Police Force reported the loss of divisional personnel file of a auxiliary police sergeant.	1	Yes	Yes	PCPD has commenced an inquiry and the Auxiliary Police Force is required to furnish more information.
Hongkong Post					
Case 12	In September 2009, a local newspaper reported that a bag of mails was placed outside a Post Office without attention.	Unknown	No	No	PCPD conducted an inquiry and was satisfied with the remedial actions taken by Hongkong Post. Case closed.

Legislative Council Panel on Information Technology and Broadcasting - Meeting on 12 July 2010

No.	Summary of the incident	Affected data subjects	Informed affected data subjects	Informed Privacy Commissioner	Actions taken / being taken by PCPD
Independent Commission Against Corruption (ICAC)					
Case 13	In July 2009, a local newspaper reported that some statement taking video tapes of ICAC were sent to a recycle company. (Same incident as per Police case (case 5))	Unknown	Unknown	No	PCPD conducted an inquiry and ICAC is required to furnish more information.
Innovation and Technology Commission (ITC)					
Case 14	In June 2010, ITC reported the loss of a CD containing personal data by a member of the Panel of Assessors.	9	No	Yes	PCPD has commenced an inquiry and ITC is required to furnish more information.
Leisure and Cultural Services Department (LCSD)					
Case 15	In April 2010, LCSD reported that 2 computers containing personal data were stolen.	404	Yes	Yes	PCPD conducted an inquiry and LCSD is required to furnish more information.

No.	Summary of the incident	Affected data subjects	Informed affected data subjects	Informed Privacy Commissioner	Actions taken / being taken by PCPD
Social Welfare Department (SWD)					
Case 16	In July 2009, SWD reported the loss of two case files containing personal data of clients and their family members.	9	Yes	Yes	PCPD conducted an inquiry and was satisfied with the remedial actions taken by SWD. Case closed.
Case 17	In August 2009, SWD reported the loss of a bank passbook of their client.	1	Yes	Yes	PCPD conducted an inquiry and was satisfied with the remedial actions taken by SWD. Case closed.
Case 18	In March 2010, SWD reported that they lost some printouts containing personal data.	126	Yes	Yes	PCPD conducted an inquiry. PCPD is examining further information submitted by SWD.
Case 19	In April 2010, SWD reported the loss of a case file containing personal data of a family.	3	Yes	Yes	PCPD conducted an inquiry. PCPD is examining further information submitted by SWD.
Case 20	In June 2010, SWD reported the loss of 2 departmental forms containing personal data of an elder and the carer of the elder.	2	Yes	Yes	PCPD is examining the incident report provided by SWD.

No.	Summary of the incident	Affected data subjects	Informed affected data subjects	Informed Privacy Commissioner	Actions taken / being taken by PCPD
University Grants Committee Secretariat (UGCS)					
Case 21	In December 2009, UGCS reported that applicants of the Research Grants Council's HK PhD Fellowship Scheme could see each other's personal data in the On-line Application System of the Scheme.	16	Yes	Yes	PCPD conducted an inquiry and UGCS is required to furnish more information.
Total	**21 Cases**	**856**			

Office of the Privacy Commissioner for Personal Data
July 2010