

**Briefing of follow-up actions on  
Suspected Loss of Registration and Electoral Office's  
Notebook Computers Containing Personal Data of Electors**

**Background**

1. During the evening of 27 March 2017 (i.e. the day following the 2017 Chief Executive Election), the Office of the Privacy Commissioner for Personal Data (“PCPD”) received a verbal notification from the Registration and Electoral Office (“REO”), stating that two notebook computers stored in the AsiaWorld-Expo, the fallback site of the 2017 Chief Executive Election, were found missing on that day. One computer contains the names of Election Committee members (“EC Members”), while the other computer contains the names, Hong Kong Identity Card numbers and addresses of about 3.78 million electors (“Electors”). The REO stated that the data had been encrypted in accordance with the relevant security requirements. The REO reported the above incident of theft to the Police early on the same day and submitted the Data Breach Notification to the PCPD on 28 March.
2. Although the case was theft in nature, the Privacy Commissioner, in consideration of the large volume of Hong Kong electors’ personal data involved, has initiated a compliance check immediately after he was being informed.

**Relevant Provisions of the Ordinance**

3. The Personal Data (Privacy) Ordinance aims at the protection of personal data privacy. As a data user, the REO is obliged to comply with the six Data Protection Principles (“DPPs”) in Schedule 1 to the Ordinance. Of direct relevance to the possible data leakage is DPP4(1). DPP4(1) provides:

*“All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorised or accidental access, processing, erasure, loss or use having particular regard to –*

- (a) the kind of data and the harm that could result if any of those things should occur;*
- (b) the physical location where the data is stored;*
- (c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data is stored;*
- (d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and*
- (e) any measures taken for ensuring the secure transmission of the data.”*

4. According to section 2(1) of the Ordinance, “practicable” means reasonably practicable.

### **The Compliance Check**

5. The Police is currently conducting a theft investigation whereas the PCPD is examining the incident from the security perspective of data protection. In the compliance check, the PCPD has made enquiries with the REO, examined the documentary evidence provided by it, and sought advice from different computer security experts to evaluate the risk of the possible data leakage.
6. The PCPD issued media statements on 27 March and 1 April to inform the public that the compliance check has been commenced and that they could lodge complaints with the PCPD if they found that their personal data was collected or used improperly. The PCPD also warned that any improper use of personal data on the electoral roll is a contravention of the current election ordinance and is a criminal offence. If members of the public find that their

personal data is misused in criminal activities such as fraud, they should report to the Police immediately.

7. The PCPD noted that on 6 April, an anonymous person, who asserted to be an elector of the Sports, Performing Arts, Culture and Publication Functional Constituency, claimed that he had received four mysterious calls enquiring him about his voting preference in the Functional Constituency Election and Election Committee Election since the REO's notebook computers containing the Electors' data had been stolen. The PCPD so far has not received any complaint from the aforesaid anonymous elector. The REO has since issued a media statement clarifying that the notebooks in question do not include telephone numbers of the electors.
8. As at 4 pm of 7 April, the PCPD received over 2003 cases, most of which came from a template provided by the appeal of 31 March 2017, "One Person, One Letter" to the PCPD, to complain against the REO and to express concerns about the possible data leakage. However, those letters do not contain substantial evidence showing leakage of any personal data, and some senders had not provided their names, contact information, etc. for the PCPD to follow up. (For the breakdown, please refer to Appendix 1).
9. The PCPD has been communicating with the REO and different computer security experts all along to follow up on the incident. The PCPD awaits further information from the REO for the earliest completion of the compliance check.
10. As not all information has been made available to the PCPD yet, it would be inappropriate for the PCPD to comment on this incident at the present stage.

**7 April 2017**

## Appendix 1

Date	Number of Cases
27/03/2017	2
28/03/2017	2
29/03/2017	11
30/03/2017	10
31/03/2017	414
01/04/2017	664
02/04/2017	393
03/04/2017	215
04/04/2017	201
05/04/2017	59
06/04/2017	25
07/04/2017 ( as at 4 pm )	7
27/03/2017 - 07/04/2017 ( as at 4 pm )	2003