Loss of Notebook Computers containing Personal Data of Election Committee Members and Electors

Chronology

The office of the Privacy Commissioner for Personal Data, Hong Kong ("**PCPD**") was verbally notified by the Registration and Electoral Office ("**REO**") on the day following the 2017 Chief Executive Election (namely 27 March 2017) that two notebook computers kept in Asia World-Expo ("**AWE**"), the fallback venue of the 2017 Chief Executive Election, were found missing on that day. The First Notebook Computer contained the names of about 1,200 Election Committee members, while the Second Notebook Computer contained the names, Hong Kong Identity Card numbers and addresses of about 3.78 million Electors (including Election Committee members). In light of the voluminous personal data involved and the wide attention in the community, the PCPD immediately conducted a compliance check on 28 March 2017.

2. After having had meeting with the officials of the REO on 10 April 2017 and obtained sufficient information, the Privacy Commissioner decided to carry out an investigation in accordance with section 38(b) of the Personal Data (Privacy) Ordinance (the "**Ordinance**") to ascertain as to whether the REO had contravened Data Protection Principle ("**DPP**") 4[1] in Schedule 1 to the Ordinance in the loss of notebook computers containing personal data of Election Committee members and electors.

3. On 12 June 2017, the PCPD completed the investigation and published the report.

---

[1] According to DPP 4(1), the REO (data user) shall take all reasonably practicable steps to ensure that personal data is protected from unauthorised or accidental access, processing, erasure, loss or use, having particular regard to a number of factors, including "*the kind of data and the harm that could result if any of those things (e.g. security incidents) should occur*".

Main Focuses of the Investigation

4. Based on the result of the compliance check, the magnitude and severity of the incident, the PCPD's investigation focused on three areas: (i) the need to store all Electors' data in the notebook computers for the Chief Executive Election; (ii) the REO's management, policies and practices in respect of personal data security; and (iii) the technical and physical security measures adopted by the REO.

5. To ensure the accuracy and the thoroughness of the investigation and impartial enforcement of the law, the Privacy Commissioner had continuously contacted the REO and sought advice of experts from Hong Kong Computer Emergency Response Team Coordination Centre, Cyber Security and Technology Crime Bureau of Hong Kong Police, and the overseas data protection authorities (e.g. Federal Trade Commission, Israeli Law, Information and Technology Authority (ILITA), the Office of the Privacy Commissioner of Canada, the Office of the Privacy Commissioner of New Zealand, the Information Commissioner's Office in United Kingdom, the Office of the Australian Information Commissioner) for verifying and examining the factual and legal issues involved.

6. On 11 April 2017, the PCPD was invited by the Panel on Constitutional Affairs to attend a special meeting for discussion of the incident. Given that the investigation was underway at that time, the PCPD craved the understanding and permission of the Panel Chairman for not attending the meeting.

Result of Investigation

7. Details of the investigation report are attached in Annex. The key results of investigation are:

(1) The PCPD's investigation revealed that the REO (i) did not fully review and evaluate the necessity and privacy risk of continuing to use and store all Electors' data in portable storage devices (such as notebook computers) for the Chief Executive Election; (ii) did not set out clear policies or internal guidelines regarding the storage of Electors' personal data in portable storage devices (including notebook computers); (iii) did not provide all staffs with detailed guidelines to protect Electors' personal data for the

Chief Executive Elections; (iv) allowed staffs to share passwords for activating the encrypted Voter Information Enquiry System and handle passwords without extreme care; and (v) had deficiencies in its physical security measures of the Fallback Venue.

The First Notebook Computer

(2) The First Notebook Computer stored the names of Election Committee members only. Such information is available to the public in the Election Committee Final Register, and could also be viewed online. As an Election Committee member's name is public data, and given that a name in itself is not considered sensitive personal data, the Privacy Commissioner takes the view that even if the names of EC members were leaked as a result of the loss of the First Notebook Computer, harm would be unlikely to be done to Election Committee members. Furthermore, the security measures (including using passwords to protect the data and storing the computer concerned in the room which was locked) taken by the REO to protect the personal data (Election Committee members' names) stored in the First Notebook Computer are considered adequate in the circumstances.

The Second Notebook Computer

(3) The Second Notebook Computer however, contained in addition to the name and address available to the public in the Final Register of Electors, the Hong Kong Identity Card number of all Electors, which is considered as sensitive personal data and not accessible by members of the public. After considering all the facts and circumstances of the case and experts' opinions, the Privacy Commissioner considers that the circumstances relating to the loss of the Second Notebook Computer are unique and unprecedented. Although the personal data of Electors involved has already undergone multiple layers of encryption and the chance of leakage is low, the loss of the Second Notebook Computer containing the personal data of all Electors could have been avoided, and hence the privacy concerns arising therefrom are understandable. The claimed effectiveness of the need for storing personal data of all Electors was not proportional to the

associated risks. The security measures adopted by the REO were not proportional to the degree of sensitivity of the data and the harm that might result from a security incident either. The result of this investigation shows that the REO lacked the requisite awareness and vigilance as expected of it in protecting personal data, rules of application and implementation of various guidelines were not clearly set out or followed, and internal communication was less than effective. Having considered all the information obtained from this investigation, the Privacy Commissioner finds that the REO failed to take all reasonably practicable steps in consideration of the actual circumstances and needs to ensure that Electors' personal data was protected from accidental loss, and hence contravened DPP 4(1) (Data Security Principle) of the Ordinance.

8. The PCPD served an enforcement notice on the REO pursuant to section 50(1) of the Ordinance to remedy and prevent any recurrence of the contravention on the day the PCPD published the investigation report. The REO is directed to: -

(1) prohibit the download or use of Geographical Constituencies electors' personal data (except their names and addresses) for the purpose of handling enquiries in Chief Executive Elections; and issue notice on this to the relevant staffs on a regular basis;

(2) set internal guidelines in respect of the processing of personal data in all election-related activities, including:

(i) technical security measures (information system encryption and password management);

(ii) physical security measures;

(iii) administrative measures on the use of notebook computers and other portable storage devices; and

(3) implement effective measures to ensure staffs' compliance with the above policies and guidelines;

(4) comply with item (1) above within 7 days after the date of service of this enforcement notice and furnish the Privacy Commissioner with the proof of compliance; and

(5) comply with items (2) and (3) above within 90 days after the date of service of this enforcement notice and furnish the Privacy Commissioner with the proof of compliance.

9. The PCPD also informed those contactable complainants [2] (approximately 1,400 in total) of the investigation result on the same day.

Follow-up work

10. The PCPD would render assistance, if required, to the REO, including training and formulating its internal guidelines.

11. The PCPD launched the Privacy Management Programme[3] in February 2014 and published the Privacy Management Programme: A Best Practice Guide to provide guiding principles to assist organisations in the development and improvement of their Privacy Management Programme according to their scope, business nature, amount and sensitivity of personal data collected and processed, etc. This guide premises on the principle of accountability, that is the best practice rather than a compulsory requirement under the Ordinance. The Government has taken the lead in undertaking to carry out the Privacy Management Programme.

12. The European Union passed the new General Data Protection Regulation ("**GDPR**") in May 2016, to be fully implemented by the member states in May 2018. The Belt and Road Initiative connects China with the Europe. With booming economic and trade development between Hong Kong and the European Union, any development of the Union's information security legislations will also have an impact on Hong Kong. The GDPR has tightened the regulations on the protection of personal information, in particular, Article 3: Extraterritorial Rights which states that when enterprises (including public organisations) provide products and services to residents in the European Union (e.g. via Internet), they have to abide by the new regulation even though the business entities are not situated in the Union.

---

[2] The PCPD received 1,968 complaints, of which over 95% (1,883) came from the same template and the content therein were almost the same, expressing their concerns over the possible leakage of their personal data. But, there was no information or evidence indicating leakage or misappropriation of Electors' personal data as a result of the loss incident. On the other hand, nearly 30% of the complaints did not bear the name and contact information of the complainants. In any event, the PCPD uploaded the Chinese and English version of the result of investigation on its website.

[3] https://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf

13. The GDPR has implemented the accountability principle, which is highlighted in this incident. It explicitly states that a data user's handling of personal data is part of its corporate governance. The GDPR requires public organisations, and data users, who engage regular and systematic monitoring of personal data on a large scale or whose major activities involve sensitive personal data, to designate a data protection officer at senior management level to coordinate and comply with the requirements of the GDPR. The GDPR also empowers data protection authorities in the member states to impose administrative fines.

14. Regarding the above issues, the PCPD will devise new guidelines and training materials on the applicability and the main issues of the GDPR, and the comparison between the GDPR and the Ordinance for all stakeholders' including public or private sectors and individual reference.

15. Moreover, between January 2016 and April 2017, the PCPD organised 50 talks, training classes, workshops and seminars on the protection of personal data for different government departments and public organisations (involving 4,751 attendees). In view of this incident, the PCPD will reallocate resources to enlarge the assistance to train the Data Protection Officers and employees of government departments.

16. Government departments should immediately start to embrace the personal data privacy protection as an integral part of their corporate governance, and implement it with a top-down approach, a shift from compliance to accountability. They should also allocate resources to train Data Protection Officers at senior management level and promote the culture of "Protect, Respect Personal Data Privacy" as an indispensable part of their corporate governance.

Office of the Privacy Commissioner for Personal Data, Hong Kong

15 June 2017

Annex

Investigation Report

(Translation)

published under Section 48(2) of the
Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong

Registration and Electoral Office

Loss of Notebook Computers containing Personal Data of Election Committee Members and Electors

Report Number：R17 – 6429

12 June 2017

Loss of Registration and Electoral Office's Notebook Computers containing Personal Data of Election Committee Members and Electors

Section 48(2) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong ("Ordinance") provides that "the *[Privacy]Commissioner [for Personal Data, Hong Kong] may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, published a report* -

(a) setting out -

(i) the result of the investigation;

(ii) any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and

(iii) such other comments arising from the investigation as he thinks fit to make; and

(b) in such manner as he thinks fit."

This investigation report is hereby published in discharge of powers and duties under section 48(2) of the Ordinance.

Stephen Kai-yi WONG
Privacy Commissioner for Personal Data, Hong Kong
12 June 2017

Investigation Report
(Translation)

(published under Section 48(2) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong)

Registration and Electoral Office

Loss of Notebook Computers containing Personal Data of Election Committee Members and Electors

Summary

The Privacy Commissioner for Personal Data, Hong Kong ("**Privacy Commissioner**") has carried out an investigation on the loss of two notebook computers containing personal data of about 1,200 Election Committee members ("**EC members**") and about 3.78 million Geographical Constituencies electors including EC members ("**Electors**") under the custody of the Registration and Electoral Office (**"REO"**) reported on the day following the 2017 Chief Executive Election (namely 27 March 2017), and publishes this report.

The first notebook computer ("**First Notebook Computer**") contained the names of EC members only. Given that the name of EC members is public data, and a name alone is not considered as sensitive personal data, the Privacy Commissioner takes the view that harm would be unlikely to be done to the EC members even when their names were leaked as a result of the loss of the First Notebook Computer. Moreover, the security measures (including using passwords to protect the data and storing the computer concerned in a locked room) taken by the REO to protect the personal data (the names of the EC members) stored in the First Notebook Computer are considered adequate. Furthermore, as the EC members could vote at the Chief Executive Election, the Privacy Commissioner considers it acceptable for the REO to download the names of the EC members to the First Notebook Computer for the purpose of recording re-issuance of name badges. In all the circumstances, the Privacy Commissioner concludes that the REO did not contravene Data Protection Principle ("**DPP**") 4(1) (Data Security Principle) of the Personal Data (Privacy) Ordinance ("**Ordinance**"), Chapter 486 of the Laws of Hong Kong, for the loss of First Notebook Computer.

The second notebook computer ("**Second Notebook Computer**") contained, in addition to the name and address available to the public in the Final Register of

Electors, the Hong Kong Identity Card number of all Electors, which is considered sensitive personal data and not accessible by members of the public. The Privacy Commissioner considers that the circumstances relating to the loss of the Second Notebook Computer are unique and unprecedented. Although the personal data of the Electors involved has already undergone multiple layers of encryption and the chance of leakage is low, the loss of the Second Notebook Computer containing the personal data of all Electors could have been avoided, and hence the privacy concerns arising therefrom are understandable. The Privacy Commissioner is of the view that the assessment and approval of the use of an enquiry system containing the Electors' data, which includes personal data not being open to the public and sensitive, was especially not well thought out or adaptive to the circumstances of the case. The REO simply followed past practices and failed to review, update or appraise the existing mechanism in a timely manner and in light of the circumstances. The claimed effectiveness of the need for storing personal data of all Electors was not proportional to the associated risks. The security measures adopted by the REO were not proportional to the degree of sensitivity of the data and the harm that might result from a data security incident either. The result of this investigation shows that the REO lacked the requisite awareness and vigilance expected of it in protecting personal data, rules of application and implementation of various guidelines were not clearly set out or followed, internal communication was less than effective, and hence failed to take all reasonably practicable steps in consideration of the actual circumstances and needs to ensure that the Electors' personal data was protected from accidental loss, thereby contravening DPP 4(1) (Data Security Principle) of the Ordinance. The Privacy Commissioner has served an Enforcement Notice on the REO pursuant to section 50(1) of the Ordinance to remedy and prevent any recurrence of the contravention.

Background

1. The office of the Privacy Commissioner for Personal Data, Hong Kong ("**PCPD**") was verbally notified by the REO on the day following the 2017 Chief Executive Election (namely 27 March 2017) that two notebook computers kept in Asia World-Expo ("**AWE**"), the fallback venue of the 2017 Chief Executive Election, were found missing on that day. The First Notebook Computer contained the names of about 1,200 EC members, while the Second Notebook Computer contained the names, Hong Kong Identity Card numbers and addresses of about 3.78 million Electors (including EC members). The REO submitted a "Data Breach Notification Form" to PCPD on 28 March 2017.

2. The Privacy Commissioner immediately followed up the reported data breach, and carried out an investigation in accordance with section 38(b)[1] of the Ordinance.

Relevant Provisions of the Ordinance

3. The Ordinance seeks to protect the privacy of individuals in relation to personal data. Generally speaking, it imposes obligations on data users (largely public and private organisations) to comply with the 6 DPPs[2] in Schedule 1 to the Ordinance.

4. Of direct relevance to the investigation is DPP 4(1) as set out in Schedule 1 to the Ordinance, which provides that:

"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 unauthorized 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."

[1] Section 38 of the Ordinance: *"Investigations by Commissioner - Where the Commissioner (a) receives a complaint; or (b) has reasonable grounds to believe that an act or practice (i) has been done or engaged in, or is being done or engaged in, as the case may be, by a data user; (ii) relates to personal data; and (iii) may be a contravention of a requirement under this Ordinance, then (i) where paragraph (a) is applicable, the Commissioner shall, subject to section 39, carry out an investigation in relation to the relevant data user to ascertain whether the act or practice specified in the complaint is a contravention of a requirement under this Ordinance; (ii) where paragraph (b) is applicable, the Commissioner may carry out an investigation in relation to the relevant data user to ascertain whether the act or practice referred to in that paragraph is a contravention of a requirement under this Ordinance."*
(https://www.elegislation.gov.hk/hk/cap486!en@2013-04-25T00:00:00/s38?elpid=153325)

[2] The 6 DPPs are: 1) Data Collection Principle; 2) Accuracy and Retention Principle; 3) Data Use Principle; 4) Data Security Principle; 5) Openness Principle; and 6) Data Access and Correction Principle. Please see Schedule 1 to the Ordinance at https://www.elegislation.gov.hk/hk/cap486!en@2013-04-25T00:00:00/sch1?elpid=228383.

5. According to section 2(1) of the Ordinance: -

"Data user" means a person who, either alone or jointly or in common with others, controls the collection, holding, processing or use of the personal data.

"Personal data" means any data relating to a living individual; in a form that can be accessed or processed; and from which it is practicable for the identity of the individual to be directly or indirectly ascertained.

"Practicable" means reasonably practicable.

Information Collected by PCPD

6. Pursuant to section 38(b) of the Ordinance, the Privacy Commissioner had reasonable grounds to believe that the REO's loss of notebook computers containing personal data might have contravened a requirement under the Ordinance and therefore carried out an investigation to ascertain whether REO had contravened the Ordinance. To ensure fair and impartial enforcement of the law, the Privacy Commissioner is mindful of the significance of the accuracy of facts.

7. In the course of handling this case, PCPD met with the representatives of the REO's Operations Division, Elections Division, Administration Division and Information Technology Management Unit; made enquiries with the REO; examined the documentary evidence provided by it and other public materials; requested the REO to perform a demonstration to PCPD and the Office of the Government Chief Information Officer ("**OGCIO**") on the procedures and technical security measures taken for accessing Electors' data; and sought professional advice from computer security experts. Below is the relevant information obtained by PCPD.

Functions of the REO and the 2017 Chief Executive Election

8. The REO provides the Electoral Affairs Commission with administrative support for the effective discharge of its statutory functions under the Electoral Affairs Commission Ordinance, Chapter 541 of the Laws of Hong Kong. The REO executes the decisions of the Electoral Affairs Commission on the delineation of geographical constituency and District Council constituency boundaries, the registration of Electors and the conduct of elections[3].

[3] See http://www.reo.gov.hk/en/about/ceo_msg.htm.

9. For the purposes of carrying out election-related activities, the REO collects, holds, processes and uses the personal data of Electors, which includes names, Hong Kong Identity Card numbers, addresses, the constituencies in which Electors are registered, telephone numbers, email addresses, fax numbers and signatures.

10. The 2017 Chief Executive Election was held on 26 March 2017. The main venue for the central polling station, central counting station and media centre was situated at the Hong Kong Convention and Exhibition Centre in Wan Chai ("**Main Venue**"), while the fallback venue was situated at the Asia World-Expo in Chek Lap Kok ("**Fallback Venue**").

11. The REO stated that it was necessary to conduct sufficient preparation work at the Fallback Venue, including arranging the computers required and ensuring that the computer systems concerned were operating normally before the polling day. In view of the relatively short polling time of the Chief Executive Election and the location of the Fallback Venue being far from the Main Venue, most of the electoral materials were prearranged at the Fallback Venue so that the polling could start at the Fallback Venue as soon as practicable.

The reported loss

12. According to the REO, the sequence of events for the reported loss is as follows: -

22 March 2017	REO staffs started preparation work at the Fallback Venue. All computer equipment (including the two notebook computers concerned) was stored in Room 107 ("**Room**") of the Fallback Venue.
23-24 March	REO staffs took the two notebook computers out of the Room for testing. The notebook computers were turned off and returned to the Room after each testing.
24 March	After the final testing, REO staffs turned off the two notebook computers, placed them on top of a paper carton box inside the Room, and then left.
25-26 March (date of the Chief Executive Election)	REO staffs patrolled and checked the Fallback Venue, but did not enter the Room.
27 March (on or about the afternoon)	When packing up equipment and materials at the Fallback Venue, REO staffs found that the two notebook computers were missing.

13. The REO reported this loss incident to the Police on 27 March 2017. The Police classified the case as theft, and their investigation is still ongoing. Up till 11 June 2017, PCPD received 92 enquiries[4] and 1,968 complaints[5]. But, there was no information or evidence indicating leakage or misappropriation of Electors' personal data as a result of the loss incident.

Personal data involved

14. According to the REO, the First Notebook Computer contained only the names of 1,194 EC members (which had already been published) in a spreadsheet with password protection. The Second Notebook Computer contained information of about 3.78 million Electors (including EC members) in the Final Register of Electors for 2016, including their names, addresses, Hong Kong Identity Card numbers and the constituencies in which they were registered, all of which were stored in an encrypted Voter Information Enquiry System ("**System**"). Neither telephone numbers nor voting records of Electors were stored in these two notebook computers.

Storing all Electors' data for the Chief Executive Election

15. The REO explained that the System was developed to allow detainees to vote. In previous Legislative Council and District Council elections, the System would be set up at dedicated polling stations in designated police stations. If a detainee requested to cast a vote on the polling day, the polling staffs of the dedicated polling station would verify his voting eligibility through the System. Given that the detainees might be the Electors of any constituencies, the System stored the information of all Electors in Hong Kong in order to facilitate the verification process.

16. In the three Chief Executive Elections in 2007, 2012 and 2017, the System was used to verify the voting eligibility of EC members who forgot to bring along their name badges and to handle any potential enquiries about Electors. If anyone had any doubt about his eligibility to vote, the REO staffs would use

[4] The enquirers mainly expressed dissatisfaction with REO; raised questions on how to protect themselves; whether it was feasible to change their Hong Kong Identity Card numbers, and the progress of PCPD's investigation, etc.

[5] 98% of the complainants raised concerns about the potential leakage of their personal data. The majority of complaints was submitted by using the complaint letter template provided on a particular social platform, the contents of which were identical.

the System to immediately check his registration particulars, explain the details of his voter registration, and answer his enquiries.

17. The REO stated that there were 6 notebook computers (including the Second Notebook Computer) installed with the System kept at the Fallback Venue. If the Fallback Venue had been activated, the Second Notebook Computer would have been placed at the counter for name badge re-issuance, whereas the other 5 computers would have been placed at the special counters and the desks of the Presiding Officer. The REO also indicated that the file containing EC members' names stored in the First Notebook Computer would be used for recording cases of re-issuing name badges to EC members who forgot to bring along their name badges.

Application and Approval procedures

18. The REO stated that the System was first used in the 2007 Chief Executive Election. However, the REO could not provide any information in relation to the approval of the use of the System in that election, or confirm whether approval had been obtained at the time.

19. Regarding the use of the System in the 2017 Chief Executive Election, the REO could only provide a draft "User Requirement" of "Polling and Counting Access Control System" sent by the Elections Division 4 Central Counting Unit[6] to the Information Technology Management Unit on 13 October 2016. This draft "User Requirement" stated that an access control system would be required, similar to that of the 2012 Chief Executive Election. One of the functions was to check the identity of EC members and to facilitate the re-issuance of name badges. However, the REO has not provided any information showing approval for using the System in the 2012 or the 2017 Chief Executive Election.

20. Aside from the authority approving the use of the System, PCPD also requested the REO to provide the approval documents in relation to the installation of the System onto notebook computers. The REO stated that the download of Electors' data to notebook computers was authorised in accordance with the REO's *"Guidelines of the Use of Computer and Information Technology Related Equipment and Services"*[7], but did not point out the relevant sections.

[6] There were four sub-divisions (1 to 4) under the Elections Division. The Elections Division 4 Central Counting Unit assisted in the preparation of the 2017 Chief Executive Election. Its duties included arranging the overall security of the main venue and venue access control.
[7] Dated 29 August 2008.

In this regard, the REO provided emails sent by Elections Division 1 Polling and Counting Station Unit[8] and Elections Division 3 Central Counting Unit[9] on 19 and 23 February 2017 respectively to the Information Technology Management Unit requesting the setup of 5 notebook computers and 1 notebook computer installed with the System at the Fallback Venue as evidence of approval.

Delivery of notebook computers and Testing records

21. The REO indicated that after the Information Technology Management Unit had prepared the relevant computer equipment according to Elections Division 4 Central Counting Unit's "User Requirements", the computers' brands, model numbers, serial numbers, REO inventory numbers and the assigned number for the election, etc. were recorded. The Information Technology Management Unit also compiled a delivery list to enumerate and inspect the computer equipment delivered to the Fallback Venue.

22. The Information Technology Management Unit performed testing on notebook computers delivered to the Fallback Venue. The testing of the Second Notebook Computer only covered the switch-on process, but there was no testing record.

23. Furthermore, the REO stated that the attendance record compiled by the Information Technology Management Unit showed that 15 staffs entered the Room between 22 and 24 March, and on 27 March 2017. There was no record showing entry to the Room by any REO staff on 25 and 26 March 2017.

REO's data security measures

24. The REO stated that the following security measures were adopted at the Fallback Venue:

Technical security measures

(i) The Electors' personal data stored in the Second Notebook Computer had been encrypted using a stringent standard which is above OGCIO's recommended class in its *"IT Security Guidelines"* [10] (details of the

[8] Elections Division 1 Polling and Counting Station Unit was mainly responsible for the arrangement of counting station.
[9] Elections Division 3 Central Counting Unit was mainly responsible for venue support for the Fallback Venue.
[10] Paragraph 12 of Version 8.0 published in December 2016.

encryption technology are not disclosed in this report given their high sensitivity; PCPD also requested the REO to demonstrate the security measures by a computer with identical settings to the Second Notebook Computer, the results of which are available in paragraph 39 below) ;

(ii) Several layers of password input were required from logging in the Second Notebook Computer, to accessing the Electors' data (details of the length and composition of the passwords are not disclosed in this report given their high sensitivity; PCPD's observations on the handling of passwords are detailed in paragraphs 56 to 57 below);

(iii) Even when the Second Notebook Computer encountered multiple unsuccessful logins, the data stored would not be automatically deleted. Instead, there would be a time delay before the next attempt was allowed, which increased from 2 to a maximum of 20 seconds for each unsuccessful login;

(iv) The REO reported at the special meeting of the Panel on Constitutional Affairs of the Legislative Council on 11 April 2017 that 5 staffs had knowledge of the passwords of the Second Notebook Computer, and subsequently confirmed it with PCPD at the meeting on 13 April 2017. At the same meeting, the REO also informed PCPD that the file containing the passwords was sent to the 5 authorised staffs by email. However, when PCPD requested a copy of that email, the REO replied that the staff who was responsible for sending that email in fact did not do so, but instead printed out the passwords and passed the print-out to another staff of the Information Technology Management Unit. The REO eventually claimed that only 2 staffs had knowledge of the passwords;

(v) The 6 notebook computers installed with the System which were kept at the Fallback Venue shared the same settings (including the passwords). The REO indicated that only the passwords of the Second Notebook Computer were changed, whereas the passwords of the remaining 5 notebook computers were retained;

(vi) On top of the two staffs of the Information Technology Management Unit mentioned in paragraph (iv) above, 6 other staffs who would work at the polling station knew the passwords of the other 5 notebook computers. The passwords were sent to one of the 6 staffs via an

encrypted email. That staff then sent the passwords to the other 4 staffs via an unencrypted email, and saved the passwords in a rearranged sequence on his mobile phone to show them to the remaining staff;

(vii) The passwords (including those of the First Notebook Computer, the Second Notebook Computer and the remaining 5 notebook computers) were not posted or displayed on the notebook computers or any objects in the Room in any way;

(viii) Staffs would shut down the notebook computers after each testing. Both the First Notebook Computer and the Second Notebook Computer were in shutdown mode when they were lost;

Physical security measures

(ix) The REO additionally arranged 34 security officers, 152 security supervisors and 275 security guards to patrol and station at the Fallback Venue during the permitted period agreed with AWE (i.e. from 22 to 28 March 2017), including arranging security guards to station in turn at the foyer outside the Room;

(x) 29 additional CCTV cameras were installed at various locations of the Fallback Venue, including the foyer outside the main door of the Room;

(xi) The Room was originally a storeroom. For the 2017 Chief Executive Election, the Room acted as the REO's server room and the office of the Information Technology Management Unit, with the main door labelled as "ITMU Office". The Room had 3 entrances, and the electronic card keys kept by the REO could open the doors of 2 entrances only, which were locked automatically at all times with the use of automatic electronic locks. The REO locked one of the entrances from the inside from 22 to 24 March, and electronic card keys were required for staffs to gain entry to the Room through the other door. The REO indicated that the remaining entrance was locked at all times by AWE;.

(xii) The REO had 2 electronic card keys, which were kept by 2 Electoral Assistants of the Information Technology Management Unit. They did not know the passwords of the notebook computers (including the Second Notebook Computer) installed with the System. Each time when an REO staff needed to enter the Room, one of the Electoral Assistants

mentioned above would accompany the staff to enter the Room. If the Electoral Assistants were out of the Room, other staffs of the Information Technology Management Unit would allow authorised persons[11] to enter the Room based on a list of authorised persons;

(xiii) Every day before and after work, the electronic card keys of the Room needed to be activated and deactivated by the control room of AWE. The REO indicated that its staffs instructed the control room to deactivate the electronic card keys of the Room after work on 24 March 2017, namely the locks could not be opened by the electronic card keys unless they were activated by the control room again; and

(xiv) The REO indicated that during office hours, staffs of the Information Technology Management Unit inside the Room would enquire visitors about their purposes of entering the Room and decide whether to allow entry. Only visitors who could provide reasonable justifications would be permitted to enter the Room, e.g. indoor phone installation, inspection of equipment in the machine room, etc. The staff would accompany the visitors for the entire period of stay to prevent the visitors from nearing the computer equipment storage area or taking photographs of the Room without permission.

25. The REO stated that it had discussed the security arrangement of the venue with AWE in the working group meetings held on 1 February and 8 March 2017. The REO also consulted the Police on the deployment of security guards and locations of CCTV cameras at the Fallback Venue, and explained the arrangement to the Police at the working group meeting on 8 March 2017.

REO's privacy management

Policies and guidelines

26. The REO stated that all staffs were required to abide by two circulars[12] in relation to personal data privacy protection, which stipulated that staffs must comply with the Ordinance, and also stated the REO's personal data policy and

[11] 38 staffs of the Information Technology Management Unit were authorised to access the Room, and their main duties were to install and test computer systems, and manage computer resources of the venue.

[12] The two circulars were "Departmental Staff Circular Memorandum No. 1/2016 - Compliance with the Personal Data (Privacy) Ordinance" (dated 7 April 2016, revised in April 2017) and "REO Administrative Circular No. 3/2006 - Administrative Procedures for Dealing with Data Holding/Access/Correction Requests on Employment-Related Personal Data" (dated 6 July 2006, revised in April 2017).

practices. One of the circulars mentioned that Hong Kong Identity Card number was sensitive personal data, and that all reasonably practicable steps should be taken to restrict access to and the processing of sensitive data on a "need-to-know" and "need-to-use" basis, so as to ensure that sensitive personal data would be protected against unauthorised or accidental access, disclosure, processing, erasure or other use. Both circulars were re-circulated every 6 months.

27. Moreover, the REO provided PCPD with *"Guidelines on Handling Personal Data of Electors and Measures of Data Protection in the Operations Division"*[13] prepared by the Operations Division, which was responsible for electors registration. The Operations Division was required to comply with these guidelines. In respect of data security, the guidelines stated that *"export of personal data should be authorized by respective section head"* and "*to avoid data leakage, users must not store personal data on portable electronic devices unless it is absolutely necessary"*. However, the REO later indicated that the guidelines did not apply to the Elections Division which was responsible for the conduct of the 2017 Chief Executive Election.

28. The REO also stated that it handled data in notebook computers according to the *"Security Regulations"*[14] (Regulations of the Government of the Hong Kong Special Administrative Region), as well as the OGCIO's *"Baseline IT Security Policy"*[15] and *"IT Security Guidelines"*[16]. The REO also issued the *"Guidelines of the Use of Computer and Information Technology Related Equipment and Services"*[17], which provided guidance on the proper use of the REO computers, as well as other information technology equipment and services.

Staff integrity and training

29. To ensure their integrity, prudence and competence, all contract staffs of the Information Technology Management Unit and those who were authorised to access Electors' data in the notebook computers were required to sign the Non-Disclosure Agreement and Joining Declaration, so as to comply with the Ordinance and the Official Secrets Ordinance, Chapter 521 of the Laws of Hong Kong, when they joined the REO.

[13] Dated 29 August 2014.
[14] Revised version published in December 2016.
[15] Version 6.0 published in December 2016.
[16] Version 8.0 published in December 2016.
[17] Dated 29 August 2008.

30. The REO provided a briefing note for staffs who were responsible for EC members' verification at the venue's entrance at the working staff general briefing session held on 15 March 2017. The briefing note stated that the System would be used for the verification of EC members' identity, and provided step-by-step guidelines on how the System should be used.

31. The REO also extracted the relevant parts on personal data protection from the Operational Manual for 2016 Legislative Council General Election and training materials for Election Committee Subsector Elections for PCPD's reference. The materials stated that if a polling officer brought along a notebook computer containing the electronic poll register on the set-up day to the polling station for testing purposes, he must safely keep the notebook computer and not leave it in the polling station until the polling day.

REO's follow-up measures

32. The REO issued a media statement to inform the public of the incident on the day when the notebook computers were found missing (i.e. 27 March 2017). The Constitutional and Mainland Affairs Bureau and the Electoral Affairs Commission also issued media statements on 27 and 28 March 2017 respectively, instructing the REO to fully assist in the Police's investigation on the loss of the notebook computers. The REO subsequently issued media statements on 28, 30 March and 6 April 2017 to respond to media enquiries, clarify the incident, and offer apologies.

33. The REO subsequently sent emails in batches from 30 March 2017 to about 550,000 electors who had provided email addresses to the REO to clarify the incident, and sent letters in batches from 31 March 2017 to the rest of the Electors to appeal to their vigilance and mitigate potential damage that might be caused by the incident.

34. Furthermore, the REO informed Government departments and relevant organisations of various sectors, including finance, insurance, telecommunications, retail, estate agents, information technology, etc., of the incident and called upon them to adopt appropriate measures to protect their own as well as their data subjects' interest.

35. The REO deleted Electors' data stored in the remaining 5 notebook computers installed with the System on 29 March 2017.

36. The Chief Electoral Officer answered questions about the incident at the special meeting of the Finance Committee of the Legislative Council held on 3 April 2017, and explained the case and the relevant follow-up measures at the special meeting of the Panel on Constitutional Affairs of the Legislative Council held on 11 April 2017.

Result of REO's preliminary review

37. The REO had conducted a preliminary review and released the result of the review together with the proposed improvement measures in the paper[18] submitted for the special meeting of Panel on Constitutional Affairs of the Legislative Council on 11 April 2017, both of which are summarised below:

(i) The System developed for detainees for use in the Legislative Council and District Council elections was not appropriate for adoption in the Chief Executive Election, as the bases of the electorate of these elections were different. In future Chief Executive Elections, the System would only store information of EC members;

(ii) There existed room for improvement concerning the storage of notebook computers at the Fallback Venue. It would be more appropriate to deliver the notebook computers to the Fallback Venue only when the fallback plan was activated;

(iii) The security arrangements of the venue, including those for the Fallback Venue, should be approved by staffs at the management level, who should also provide sufficient guidelines and directions to the front-line staffs so as to ensure that all security arrangements would be properly carried out; and

(iv) The REO would work with relevant departments and comprehensively review its arrangements on the collection, use, processing and storing of the personal information of Electors, system requirements, the overall security arrangements, etc. The REO would fully implement PCPD's proposed improvement measures and recommendations.

[18] The document may be viewed in its entirety at the following link:
http://www.legco.gov.hk/yr16-17/english/panels/ca/papers/ca20170411cb2-1167-1-e.pdf

Examination of computer settings

38. On 13 April 2017, the REO demonstrated, at PCPD's request, the procedure of accessing Electors' data and other relevant security measures using a notebook computer with the same settings as those of the Second Notebook Computer, for PCPD to evaluate the computer security technology adopted. Considering the risk that would be brought about by the disclosure of the security technology (e.g. brand of the encryption software, composition of passwords, data access procedures, etc.), PCPD only invited experts from the OGCIO to attend the demonstration, and requested them to raise questions to the REO and offer professional advice on site.

39. Having considered the Government's internal security as well as public interest, the Privacy Commissioner decides to disclose the following findings derived from the examination of computer settings, the comments from the OGCIO and the supplementary information provided by the REO: -

(i) Users of the notebook computers were required to go through several programmes before they were allowed to access Electors' data, which was protected by multiple encryption layers;

(ii) The strongest layer appeared to have met the industrial standard (i.e. satisfying the requirements of strong encryption). Decryption could only be carried out by brute force attacks[19] on the passwords, and using general commercial computers to crack the encryption formula would take hundreds of years;

(iii) For every unsuccessful login after inputting the wrong passwords, the protection layer would delay the login time so as to strengthen the difficulty of decryption. In other words, the protection layer would respond slowly and the decryption time would be lengthened even when a supercomputer was used to attack the passwords. Consequently, compromising the passwords would be a matter of sheer luck;

(iv) Two-factor authentication was not adopted for accessing the Electors' data. In other words, one would only need to input several sets of correct passwords to open the System to access the data without using

[19] According to the InfoSec website managed by the OGCIO, a brute-force attack is defined as a technique used to break an encryption or authentication system by trying all possibilities. (https://www.infosec.gov.hk/english/glossary/glossary_b.html)

another tool such as an electronic certificate, security token or mobile phone;

(v) The System would not show more than one Elector's data at the same time even when accessed. In other words, in the event that a valid Hong Kong Identity Card number of an Elector was successfully inputted, the System would only show the data of that Elector; and

(vi) Hong Kong Identity Card numbers were encrypted before being stored in the System, while other personal data was stored in plain text.

The Law and Findings of the Investigation

40. According to DPP 4(1), the REO (data user) shall take all reasonably practicable steps to ensure that personal data is protected from unauthorised or accidental access, processing, erasure, loss[20] or use, having particular regard to a number of factors, including *"the kind of data and the harm that could result if any of those things (e.g. security incidents) should occur"*. In other words, the security measures adopted by a data user should be proportionate to the degree of sensitivity of the data and the harm that may result from a security incident. "Harm" is not limited to the harm done to the personal data privacy of data subjects (Electors), but extends to include all sorts of other harm arising out of the personal data privacy invasion.

41. DPP 4 does not call for the REO's absolute guarantee on personal data security. The loss of personal data merely due to the loss of storage device does not automatically mean that the REO had contravened DPP 4. On the contrary, though there is no direct evidence showing that the personal data has fallen into the hands of a third party, the Privacy Commissioner still needs to consider the security measures adopted by the REO in the incident before determining whether it contravened DPP 4.

42. As the subject of PCPD's investigation is the REO and not individual staffs, and given that the REO has already provided PCPD with internal policies and guidelines on personal data protection, any follow-ups taken by the REO would not affect the Privacy Commissioner's decisions in this case.

[20] The term "loss" was introduced by the Personal Data (Privacy) (Amendment) Ordinance 2012, which explicitly requires data users to adopt corresponding security measures to prevent the loss of personal data.

(A) The First Notebook Computer

43. The First Notebook Computer stored the names of EC members only. Such information is available to the public in the Election Committee Final Register, and could also be viewed online[21]. As an EC member's name is public data, and given that a name in itself is not considered sensitive personal data, the Privacy Commissioner takes the view that even if the names of EC members were leaked as a result of the loss of the First Notebook Computer, harm would be unlikely to be done to EC members. Furthermore, the security measures (including using passwords to protect the data and storing the computer concerned in the Room which was locked) taken by the REO to protect the personal data (EC members' names) stored in the First Notebook Computer are considered adequate in the circumstances.

44. Moreover, as EC members could vote at the Chief Executive Election, the Privacy Commissioner considers it acceptable to download the names of EC members to the First Notebook Computer for the purpose of recording the re-issuance of name badges.

45. In all the circumstances of the case, the Privacy Commissioner concludes that the REO did not contravene DPP 4(1) (Data Security Principle) of Schedule 1 to the Ordinance for the loss of the First Notebook Computer containing personal data of EC members.

(B) The Second Notebook Computer

46. The Second Notebook Computer however, contained in addition to the name and address available to the public in the Final Register of Electors, the Hong Kong Identity Card number of all Electors, which is considered as sensitive

[21] EC members' names can be viewed on the following links:
(1) The names of EC Members from subsector elections can be viewed at the webpage of "2016 Election Committee Subsector Elections" (http://www.elections.gov.hk/ecss2016/eng/results.html?1496836412947)
(2) The names of EC Members nominated by the religious subsector can be viewed at the government press release dated 12 December 2016 (http://www.info.gov.hk/gia/general/201612/12/P2016120900771.htm?fontSize=1)
(3) The names of all ex-officio members of the Election Committee (the Hong Kong deputies to the National People's Congress and members of the Legislative Council) can be viewed at the websites of the National People's Congress (http://www.npc.gov.cn/npc/gadbzl/xgdbzl_11/node_8514.htm in Chinese only) and Legislative Council (http://www.legco.gov.hk/general/english/members/memberslist/precedence/sixthlegislativecouncil_2016_2020.pdf).

personal data and not accessible by members of the public. The Electors would suffer serious harm if culprits obtain the data, including fraud by misappropriating their identity. Hence, this investigation should focus on: (i) the need to store all Electors' data in the notebook computers for the Chief Executive Election; (ii) the REO's management, policies and practices in respect of personal data security; and (iii) the technical and physical security measures adopted by the REO.

(i) The need to store all Electors' data in the notebook computers for the Chief Executive Election

47. The System contained about 3.78 million Electors' personal data, including Hong Kong Identity Card number which is considered sensitive. The Privacy Commissioner considers that the REO should be prudent and vigilant as expected of it when approving the use of the System and the download of it onto the notebook computers, which are vulnerable to loss. The REO should also evaluate and appraise the need for such download. Otherwise, it should not be deemed to have taken all the reasonably practicable steps to protect Electors' personal data. If there is no sufficient justification for the download, the REO should refrain from doing so in order to minimise the risk of data leakage.

48. Noting that the System has been in use in the Chief Executive Elections since the 2007, PCPD requested the REO to provide authority in relation to the approval for downloading all Electors' personal data to notebook computers, evidence concerning evaluation of the necessity of the download, as well as guidelines on the relevant approval(s). The Privacy Commissioner is taken aback by the REO not being able to provide any information or proof of approval for using the System, or even confirm that such use was approved at all.

49. Similarly, in respect of the preparation for the 2017 Chief Executive Election, the REO could only provide an email relating to the draft "User Requirement" of "Polling and Counting Access Control System". However, this draft document did not appear to explicitly state the need for the use of the System, but only mentioned that the arrangements would have to make reference to those of the 2012 Chief Executive Election. The Information Technology Management Unit provided notebook computers installed with the System when asked to arrange for the required computer equipment. The emails sent by the relevant units of the Elections Division to the Information Technology

Management Unit requesting for computer equipment at the Main Venue and Fallback Venue showed that a total of 21 staffs, including Senior Electoral Officers at the supervisory rank, had knowledge of the use of notebook computers installed with the System.

50. The REO stated that the download of Electors' data to notebook computers was authorised in accordance with the REO's *"Guidelines of the Use of Computer and Information Technology Related Equipment and Services"*. PCPD read the Guidelines and considered that the relevant guidelines might include: *"without prior approval from the relevant unit head, no sensitive information could be brought away from the office", "without prior approval from the relevant unit head, no computer equipment, devices or accessories could be brought away from the office" or "...request for extracting specific information should be submitted by Executive Officer II or Electoral Assistant or above via unit head to the head of the Information Technology Management Unit, together with the justifications"*. There was however no mention of the conditions for the download of all Electors' data to notebook computers.

51. From the facts and information gathered from the REO, the Privacy Commissioner is of the view that the assessment and approval of the use of an enquiry system containing Electors' data, which includes personal data not being open to the public and sensitive, was especially not well thought out or adaptive to the special circumstances of the case. The REO simply followed past practices and failed to review, update or appraise the existing mechanisms in a timely manner and in light of the circumstances.

52. On the question of why all Electors' data was needed for the Chief Executive Election where only 1,194 EC members were eligible to vote, the REO explained that the data would be used to verify the voting eligibility of EC members and handle enquiries about Electors. The Privacy Commissioner is of the opinion that although these might be reasonable and legal purposes generally, bringing all Electors' data for the Chief Executive Election is a disproportionate and imbalanced act.

53. As the REO had already had an online voter information enquiry system, it could have used it for accessing information to answer enquiries or provide the website link for the enquirers' reference without having to resort to data stored in notebook computers.

(ii) Management, Policies and Practices of personal data security

54. The two circulars[22] concerning privacy protection of the REO only reminded staffs to comply with the requirements of the Ordinance and stated briefly the REO's personal data policy and practices. However, the REO did not set out clear policies or internal guidelines on the storage of Electors' personal data in notebook computers and the protection measures needed to be adopted for the Chief Executive Elections.

(iii) Technical and Physical security measures

55. The REO stressed that the data had undergone multiple encryptions, and was therefore difficult to crack. The Privacy Commissioner acknowledges that the encryption standard adopted is recognised by the National Institute of Standards and Technology of the United States, and is used by the United States Government agencies[23]. Based on the REO's replies and demonstration, the Privacy Commissioner considers that the REO adopted technology of reasonable standard to encrypt Electors' data, the relevant programme and the System.

56. PCPD noted that the REO did not follow the password requirements stipulated in its *"Guidelines of the Use of Computer and Information Technology Related Equipment and Services"* and the OGCIO's "*IT Security Guidelines*" [24]. Despite such non-compliance, the REO's information nevertheless showed that the passwords were not simple or easy to crack. Before the name, address and constituency of an Elector are shown, the setting of the System requires the correct input of password followed by the valid Hong Kong Identity Card number of the Elector. In other words, unauthorised persons need to acquire the correct passwords as well as the valid Hong Kong Identity Card number of an Elector before they can access that Elector's data and that Elector's data only. There is also a time delay for each unsuccessful login. The Privacy Commissioner therefore accepts that the encryption technology and the system setup adopted by the REO makes it enormously difficult and time-consuming for unauthorised persons to access all Electors' data.

[22] Please refer to footnote 12 for the full title of the circulars.
[23] The National Institute of Standards and Technology Special Publication 800-131A Revision 1 is available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf
[24] Paragraph 11.4(c) of Ver 8.0 dated December 2016.

57. Despite the above technical security measures, the ways the REO handled the passwords of notebook computers undermined their effectiveness. The Privacy Commissioner considers that sharing of passwords would make it impossible for the REO to ascertain who accessed the data. Using unencrypted emails to circulate passwords also increased the risk of leaking the passwords. The Privacy Commissioner also considers that it would have been practicable for the REO to assign different passwords to individual staffs and provide guidelines requiring them to transmit passwords through more reliable means, but the REO did not do so.

58. The Privacy Commissioner notes that the REO adopted certain physical security measures, including locking the Room, arranging security guards to station in turn at the foyer of the Room, installing additional CCTV cameras at the foyer outside the main door of the Room, and seeking advice from the Police on physical security measures of the Room.

59. However, the Privacy Commissioner also finds that the entrances of the Room were not within the range of the CCTV cameras, the REO did not keep the access record to the Room, the 2 notebook computers lost were simply placed on top of a paper carton box instead of being locked in a steel cabinet, which was what the REO did at the Main Venue. The Privacy Commissioner takes the view that the REO did not fully take into account the importance and sensitivity of the personal data when devising the physical security measures of the Room.

60. After its preliminary review, the REO conceded that it would have been more appropriate to deliver the notebook computers to the Fallback Venue only when the fallback plan had been activated. The security arrangements of the venue should have been approved by the management staff, who should also provide sufficient guidelines and directions to the front-line staffs so as to ensure that all security arrangements were properly carried out. Moreover, there were suggestions for stricter measures including locking the notebook computers in a cabinet inside a locked room, stationing 24-hour security personnel to guard the Room, recording access to the Room, installing remote data wipe application to notebook computers, etc. The Privacy Commissioner welcomes the REO's improvement measures and any recommendations for enhancing personal data protection.

61. The investigation regarding the loss of the Second Notebook Computer revealed that the REO (i) did not fully review and evaluate the necessity and

privacy risk of continuing to use and store all Electors' data in portable storage devices (such as notebook computers) for the Chief Executive Election; (ii) did not set out clear policies or internal guidelines regarding the storage of Electors' personal data in portable storage devices (including notebook computers); (iii) did not provide all staffs with detailed guidelines to protect Electors' personal data for the Chief Executive Elections; (iv) allowed staffs to share passwords for activating the System and handle passwords without extreme care; and (v) had deficiencies in its physical security measures of the Fallback Venue.

62. After considering all the facts and circumstances of the case and experts' opinions, the Privacy Commissioner considers that the circumstances relating to the loss of the Second Notebook Computer are unique and unprecedented. Although the personal data of Electors involved has already undergone multiple layers of encryption and the chance of leakage is low, the loss of the Second Notebook Computer containing the personal data of all Electors could have been avoided, and hence the privacy concerns arising therefrom are understandable. The claimed effectiveness of the need for storing personal data of all Electors was not proportional to the associated risks[25]. The security measures adopted by the REO were not proportional to the degree of sensitivity of the data and the harm that might result from a security incident either. The result of this investigation shows that the REO lacked the requisite awareness and vigilance as expected of it in protecting personal data, rules of application and implementation of various guidelines were not clearly set out or followed, and internal communication was less than effective. . Having considered all the information obtained from this investigation, the Privacy Commissioner finds that the REO failed to take all reasonably practicable steps in consideration of the actual circumstances and needs to ensure that Electors' personal data was protected from accidental loss, and hence contravened DPP 4(1) (Data Security Principle) of the Ordinance.

[25] See the principle of proportionality as explained in *Attorney General of Hong Kong v Lee Kwong-Kut* [1993] AC 951, (Privy Council); *HKSAR v LAM Hon Kwok Popy* CACC 528/2004, 21 July 2006; *Hysan Development Co. Ltd. and Others v Town Planning Board* FACV 21/ 2015, 26 September 2016 (Court of Final Appeal).

Enforcement Notice

63. Pursuant to section 50(1) of the Ordinance and in consequence of an investigation, if the Privacy Commissioner is of the opinion that the relevant data user is contravening or has contravened a requirement under the Ordinance, the Privacy Commissioner may serve on the data user a notice in writing, directing the data user to remedy and, if appropriate, prevent recurrence of the contravention.

64. In view of the Privacy Commissioner's finding of contravention on the part of the REO regarding the handling of the Second Notebook Computer involving personal data, the Privacy Commissioner has decided to serve an enforcement notice on the REO pursuant to section 50(1) of the Ordinance to remedy and prevent any recurrence of the contravention. The REO is directed to: -

(i) prohibit the download or use of Geographical Constituencies electors' personal data (except their names and addresses) for the purpose of handling enquiries in Chief Executive Elections; and issue notice on this to the relevant staffs on a regular basis;

(ii) set internal guidelines in respect of the processing of personal data in all election-related activities, including:
   (a) technical security measures (information system encryption and password management);
   (b) physical security measures;
   (c) administrative measures on the use of notebook computers and other portable storage devices; and

(iii) implement effective measures to ensure staffs' compliance with the above policies and guidelines.

Recommendations

65. Having considered all the circumstances of the case, the Privacy Commissioner makes the following 11 recommendations: -

Use only "necessary" personal data in different elections

(i) When conducting all election-related activities, the REO should only make available the personal data for access or use on a "need-to-know" and "need-to-use" basis so as to minimise the risk of data breach, especially when portable storage devices such as notebook computers are involved. Furthermore, the REO should adopt the principle of least-privileged rights, by which only staffs authorised to handle identity verification would be able to retrieve or access relevant personal data;

Strictly review, approve and monitor the download and copying of systems containing Electors' personal data

(ii) The REO should strictly evaluate the necessity of downloading and copying systems containing Electors' personal data and set approval procedures and standards;

(iii) The REO should monitor if any system containing Electors' personal data has been downloaded or copied without authorisation. Such systems and the related servers should record all activity logs. Whenever a system user accesses, uses, downloads, edits and/or deletes the data, the REO should be able to trace the logs;

(iv) The REO should install monitoring and alarm mechanisms in all the systems containing the Electors' personal data and the related servers, so that whenever there is any irregularity (e.g. download or deletion of huge personal data), timely reporting of the case, as well as tracing and reviews can be done;

Adopt effective technical security measures when storing Electors' personal data

(v) As storing personal data in notebook computers or portable storage devices will pose high risk to information security, personal data should not be stored in notebook computers or portable storage devices unless absolutely necessary;

(vi) If it is necessary to store the Electors' personal data in notebook computers or other portable storage devices, the REO should adopt effective technical security measures according to the quantity and

sensitivity of the data, e.g. two-factor authentication in data access, automatic system lock or automatic data wipe upon several times of unsuccessful login, installation of location tracking software, etc.;

Formulate, systematically review and update personal data security policy

(vii) In addition to complying with relevant policies of the Government and the OGCIO, the REO should formulate, systematically review and update its current personal data security policies and practical guidelines (including on-line and off-line) according to its functions and activities to ensure that the information on handling the Electors' personal data is up-to-date;

(viii) The REO should effectively disseminate the personal data security policies to all staffs to ensure that they know and understand the policies and requirements. Clear ways to access the relevant information promptly should also be provided;

(ix) The REO should review and formulate a regular and systematic compliance check mechanism to ensure compliance with the personal data security policies, procedures and practical guidelines;

Conduct Privacy Impact Assessment

(x) Before commencement of any new task or project involving the creation, collection, use or storage of voluminous Electors' data, sensitive one in particular, is involved, the REO should carry out a privacy impact assessment[26]. The REO should adopt adequate security measures to address the privacy risks arising from the project. The assessment procedures and steps should be clearly recorded and filed; and

Implement Privacy Management Programme

(xi) In 2014, the Government (including all bureaux and departments) undertook to implement the Privacy Management Programme[27] to embrace personal data privacy protection as part of their corporate

[26] PCPD's information leaflet on "Privacy Impact Assessment" can be downloaded via the following link: https://www.pcpd.org.hk/english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf

[27] PCPD's "Privacy Management Programme: A Best Practice Guide" can be downloaded via the following link: https://www.pcpd.org.hk/pmp/files/PMP_guide_e.pdf

governance responsibilities. The Privacy Commissioner strongly recommends that the REO should learn from the lessons of the incident and adopt the programme as a top-down organisational imperative. The REO should review and update its programme controls (including personal data inventory, policies, risk assessment tools, training and education requirements, breach handling, etc.) and raise staffs' awareness and vigilance in protecting protecting and respecting the Electors' personal data privacy with a view to complying with the Ordinance effectively and regaining the confidence and trust of the Electors.

The office of the Privacy Commissioner for Personal Data, Hong Kong
12 June 2017