Investigation Report

Published under Section 48(2) of the Personal Data (Privacy) Ordinance (Cap 486)

Registration and Electoral Office

Two Personal Data Breach Incidents

Report Number：R22 - 4116

Date Issued: 29 December 2022

Investigation Report
Registration and Electoral Office
Two Personal Data Breach Incidents

Section 48(2) of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance) provides that "*the* [Privacy Commissioner for Personal Data] *may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, publish 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 the exercise of the powers conferred under section 48(2) of the Ordinance.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
29 December 2022

Investigation Case (1) – A staff member of the Registration and Electoral Office wrongly dispatched files containing data of electors to an unknown recipient through email

Background

1. On 24 March 2022, the Registration and Electoral Office (the REO) submitted a data breach notification to the Office of the Privacy Commissioner for Personal Data (the PCPD) reporting that a staff member had mistakenly sent files containing registration particulars of about 15,000 electors to an unknown email address on 23 March 2022 (Incident 1). The files concerned contained Chinese and English names of the electors as well as their residential addresses.

2. The REO reported Incident 1 to the Electoral Affairs Commission, the Constitutional and Mainland Affairs Bureau (the CMAB), the Office of the Government Chief Information Officer (the OGCIO) and the Police on the same date and issued a press release[1] giving the public an account of the incident on 25 March 2022.

3. Upon receipt of the aforesaid data breach notification, the Privacy Commissioner for Personal Data, Hong Kong (the Commissioner) commenced an investigation against the REO on 6 April 2022 pursuant to section 38(b)[2] of the Personal Data (Privacy) Ordinance, Chapter 486, Laws of Hong Kong (the Ordinance) in relation to Incident 1 to ascertain whether the relevant act of the REO in Incident 1 is in contravention of the requirements under the Ordinance.

[1] https://www.info.gov.hk/gia/general/202203/25/P2022032500609.htm?fontSize=1

[2] Section 38(b) the Ordinance provides that where the Commissioner has reasonable grounds to believe that an act or practice has been done or engaged in, or is being done or engaged in by a data user which relates to personal data and may be a contravention of a requirement under the Ordinance, the Commissioner may carry out an investigation in relation to the relevant data user to ascertain whether the act or practice is a contravention of a requirement under the Ordinance.

Information Obtained from the Investigation

4. During the course of the investigation, the Commissioner reviewed and considered the information provided by the REO in relation to Incident 1, including an internal investigation report provided by the REO and a summary investigation report published by the REO on 13 September 2022[3]. The Commissioner also considered the follow-up and remedial actions taken by the REO in the wake of Incident 1.

5. On the other hand, representatives from the OGCIO, the CMAB and the REO formed a working group (the Working Group) and conducted a comprehensive review on the information security of the REO from April to June 2022. Upon completion of the review, the OGCIO provided the REO with a review report (the Review Report) setting out recommendations on enhancing the cyber security level and the resilience against cyber risks of the REO. Although the primary purpose of the Review Report was to provide recommendations on the overall information security of the REO rather than to identify deficiencies on the part of the REO in Incident 1, the Commissioner also considered the contents of the Review Report in the course of the investigation.

Background and Occurrence of Incident 1

6. According to the information provided by the REO, the staff member involved in Incident 1 was a Clerical Officer (the Clerical Officer) under the Geographical Constituency Vetting Team of the Voter Registration Division of the REO. One of her main duties was to lead her team to conduct data matching exercises with other Government departments.

[3] https://www.reo.gov.hk/pdf/incident_report/Summary_Report_data_breach_incident_March2022(Eng).pdf

7. Records involved in Incident 1 concerned information of electors whose tenancy agreements in public housing estates had been terminated as provided by the Housing Department. Upon receipt of the information from the Housing Department, the REO would conduct cross-checking by comparing the residential addresses of the electors in the possession of the REO with those provided by the Housing Department. If the addresses of an individual elector in the two data sets are identical, the REO would have a reasonable doubt that the registered residential address of the elector is no longer his/her only or principal residential address, and he/she would be subject to inquiry procedures pursuant to the relevant laws[4]. In Incident 1, the subordinates of the Clerical Officer completed the first checking and passed the relevant data to the Clerical Officer for the second checking.

8. Incident 1 occurred during the period when the fifth wave of COVID-19 ran rampant. From 25 January 2022, the REO put in place special work-from-home arrangements by dividing staff into different teams to work at home alternately to reduce social contact. In the circumstances, the REO provided some of its staff members with laptop computers equipped with virtual private networks to allow them to log onto the REO's system when they worked from home. Although the Clerical Officer was arranged to work from home on certain days, she was not provided with a laptop computer as her work involved the handling of a large amount of personal data, and she was only permitted to perform the tasks relating to data matching with her computer workstation in the office.

9. At 7:03 p.m. on 23 March 2022, the Clerical Officer planned to send two Excel files which contained the data of electors (the Two Excel Files) to her personal email account to facilitate her work from home on the next day. However, she mistakenly inputted an incorrect email address so that the Two Excel Files were sent to an unknown recipient. The Clerical

[4] Section 7 of the Electoral Affairs Commission (Registration of Electors) (Legislative Council Geographical Constituencies) (District Council Constituencies) Regulation (Cap. 541A).

Officer only realised the mistake when she noticed that the email did not reach her personal email account after some 10 minutes. She immediately reported the matter to the Assistant Electoral Officer who was responsible for the final checking. The Assistant Electoral Officer only reported the incident to the REO in the morning of 24 March 2022.

10. After the Clerical Officer provided statements to the Police, the REO further noted that the Clerical Officer had in fact sent two other emails containing data of electors to her personal email account on the date of the incident. The Clerical Officer sent an email containing data of about 1,000 electors (including the English and Chinese names and internal reference numbers which could not be used for identifying an individual) at 5:43 p.m. After realising that the Two Excel File had been wrongly sent to the unknown recipient, the Clerical Officer sent the Two Excel Files to her personal email account again at 7:58 p.m. to facilitate her work from home on the next day.

Personal Data Affected

11. Under section 2(1) of the Ordinance, "personal data" means any data relating directly or indirectly to a living individual, from which it is practicable for the identity of the individual to be directly or indirectly ascertained, and in a form in which access to or processing of the data is practicable.

12. The Two Excel Files contained data of 15,070 electors[5] (data of 5,264 and 9,806 electors were contained in the Two Excel Files respectively), including their names and residential addresses in the public housing units the tenancy agreements of which had been terminated as provided by the Housing Department, as well as the names and registered addresses of these electors contained in the REO's records.

[5] After excluding 103 deceased electors, the total number of affected data subjects was 14,967.

Explanation by the Clerical Officer in relation to Incident 1

13. The Clerical Officer stated that due to the implementation of the work-from-home arrangement, her working hours in the office were reduced. In order not to delay work progress, she therefore sent some work-related information through her official email account to her personal email account on 23 March 2022, including the Two Excel Files. The Clerical Officer indicated that the Two Excel Files were not password protected.

14. The Clerical Officer explained that the email address of the personal email account that she originally intended to use was in the format of xyzxyz0000@gmail.com[6], but she wrongly inputted an email address in the format of xyzabcde11@gmail.com. This error occurred because she has another email account in the format of xyzabcde11@hotmail.com.

15. The Clerical Officer stated that she had been working at the REO for about 26 years and knew at the time of the incident that the sending of files containing the data of electors to personal email account is not allowed. She admitted that she had arranged for the files to be sent to her personal email account in the heat of the moment, which led to the incident. The Clerical Officer confirmed that all files containing the data of electors (including the Two Excel Files) had been deleted from her personal email account.

REO's Investigation Findings

16. According to the REO's internal investigation report, the REO had internal procedures and guidelines in relation to the protection of personal data of electors. In Incident 1, the Clerical Officer failed to comply with the

[6] The formats of the email addresses described in this paragraph are not real email addresses.

guidelines[7] set out in the annex to the REO Administrative Circular No. 7/2017 (Departmental Information Technology Security Policy and the Departmental Information Technology Security Guidelines and Procedures), which stipulates that "*only use the email system of REO for transmission of classified information through email*" and "*don't use personal email accounts for official duties or for transmitting classified information or personal data*". The REO stated that the aforementioned circular would be recirculated to all staff members every six months. The last recirculation before Incident 1 was made on 1 March 2022. In addition to the aforementioned circular, the REO indicated that the Clerical Officer had also watched videos on data protection.

17. The REO concluded in its internal investigation report that the Clerical Officer had committed misconduct of negligence in handling personal data and contravened departmental guidelines on information technology security. The REO considered that the incident amounted to a serious data breach incident given the large amount of data of electors involved, and the Clerical Officer should be personally held responsible for the incident. The REO stated that it has been taking follow-up action on the Clerical Officer's misconduct under the existing civil service disciplinary mechanism.

REO's Follow-up Actions and Improvement Measures

18. After becoming aware of Incident 1, the REO immediately sent an email to the unknown recipient on 24 March 2022 requesting immediate and permanent deletion of the Two Excel Files and asked the recipient to contact the REO for follow-up. The REO also reported the incident to the PCPD, the Electoral Affairs Commission, the CMAB, the OGCIO, and the Police on the same date. The REO issued a press release giving the public

[7] "Dos and DON'Ts"

an account of the incident on 25 March 2022[8] and informed the affected electors of the incident in writing on 31 March 2022.

19. The Police had later successfully contacted the unknown recipient and confirmed that the recipient had not opened the concerned email containing the data of electors and had deleted the email.

20. To strengthen data security and prevent recurrence of similar incidents, the REO has imposed technological restrictions concerning information security on staff of the relevant divisions from April 2022. Unless there is a genuine operational need, staff at the rank below Assistant Electoral Officer cannot send out emails to personal email accounts through the departmental email system, and their computer also cannot access the websites of Internet email service providers commonly used in Hong Kong.

21. After the completion of the comprehensive review on the information security of the REO by the Working Group, the OGCIO provided the REO with the Review Report which offered substantial advice in relation to information security management, awareness and training on information security, system security and extra protection on IT facilities. The REO has undertaken to prioritise the implementation of the Working Group's recommendations and apply for the required financial and staffing resources.

Findings and Contravention

<u>The REO as the data user in Incident 1</u>

22. The major functions of the REO include the handling of voters' registration and election related matters in Hong Kong. In exercising these functions,

[8] See footnote 1.

the REO would collect, hold, process, and use the personal data of electors. In this regard, the REO is the data user[9] as defined under section 2(1) of the Ordinance and is required to comply with the requirements of the Ordinance, including the six Data Protection Principles (DPPs) set out in Schedule 1 to the Ordinance.

Data Protection Principle 4(1)

23. DPP4(1) in Schedule 1 to the Ordinance stipulates that a data user is obliged to take all practicable steps to ensure that the personal data held by it is 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.

24. Having considered the facts of Incident 1 and evidence obtained during the course of the investigation, the Commissioner considers that the following reasons had led to the occurrence of Incident 1: -

(1) Failure of staff to comply with the guidelines in the relevant departmental circular on information technology security

[9] Under section 2(1) of the Ordinance, a data user, in relation to personal data, means "*a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data*".

25. The Clerical Officer failed to comply with the guidelines set out in Administrative Circular No. 7/2017 on "Departmental Information Technology Security Policy and the Departmental Information Technology Security Guidelines and Procedures", which stipulates that "[staff should] *only use the email system of REO for transmission of classified information through email*" and "[staff should not] *use personal email accounts for official duties or for transmitting classified information or personal data*", and sent emails containing the data of electors on three separate occasions to her personal email account on the date of the incident, including the instance where the Two Excel Files were wrongly sent to the unknown recipient, which caused this data breach incident.

26. In addition, after discovering that the email concerned had been sent to an unknown recipient by mistake, the Clerical Officer, without thorough consideration, still sent the Two Excel files to her personal email account again to facilitate her work from home on the next day. This act was a complete disregard of the REO's prescribed guidelines.

(2) Inadequate awareness of data protection

27. The Clerical Officer not only failed to comply with the relevant guidelines set out in the departmental circular, but also demonstrated a serious lack of awareness to protect personal data: -

(i) The Clerical Officer, without thorough consideration of the security risks involved, negligently sent emails which contained a large number of personal data to an email address outside the REO's email system and did not do anything to protect the files concerned (e.g. by encrypting or password-protecting the files);

(ii) The Clerical Officer failed to exercise due care to carefully check the email address of the recipient (i.e. her personal email address) before sending out the email in question; and

(iii) After realising that the email in question had been wrongly sent to an unknown recipient, the Clerical Officer did not cease to send the relevant data but proceeded to send the same email containing the Two Excel Files the second time to her personal email account to facilitate her work at home.

28. The REO submitted to the Commissioner that circulars in data protection had been distributed to the Clerical Officer prior to the incident, and she had watched videos on data protection. Apparently, these trainings were ineffective in bringing the level of data protection awareness of that staff member who has served at the REO for 26 years to an acceptable standard.

29. The Commissioner noted that the OGCIO gave two recommendations on education and training relating to information security to the REO in the Review Report, including establishing a working group on information security awareness and training to formulate plans for establishing an information security awareness programme, and expanding the variety and delivery channels of information security awareness activities, to help develop a positive information security culture. In the circumstances, there appears to be inadequacies the information security education and training of the REO.

(3) Inadequate information security measures of the REO

30. The REO did not put in place appropriate technological security restrictions at the time of the incident to prohibit staff below the rank of Assistant Electoral Officer (including the Clerical Officer) from sending

out emails to personal email accounts through their official email accounts. The REO only adopted the aforementioned technological security measures after the incident as remedial measures. In addition, the REO did not adopt any security measures, such as data loss protection tools, to detect and stop any emails and attachments containing personal data from being sent to email accounts outside the email system of the REO.

31. Apparently, given that the REO holds and routinely processes personal data of over millions of electors, the incident could have been avoided if the REO had assigned authorities of sending emails to external parties based on the roles and responsibilities of staff, and adopted appropriate security measures to detect and stop any emails and attachments containing personal data from being sent to email accounts outside the email system of the REO.

Conclusion – Contravention of DPP4(1)

32. Having considered all the evidence in this case, **the Commissioner considers that Incident 1 mainly involved human errors. The data breach incident stemmed from the negligence and lack of awareness of an individual staff member of the REO to data protection, which led to the contravention of the relevant departmental guidelines of the REO on information technology security. Simply to facilitate her work at home, the staff member concerned sent an email which contained a huge amount of personal data of electors to an incorrect email address outside the REO's email system with neither thorough consideration of the security risks involved nor careful checking of the email address of the recipient.**

33. **On the other hand, the Commissioner considers that given that the REO holds and processes a large amount of personal data of electors, it ought to adopt more stringent information security measures to**

ensure that its systems could adequately deal with staff negligence or inappropriate conduct. However, the REO had not put in place appropriate information security measures prior to the incident, which allowed its staff to use its email system to freely send files which contained personal data to personal email addresses outside the email system of the REO. This was another root cause of Incident 1.

34. **In the circumstances, the Commissioner considers that the REO had not taken all practicable steps in Incident 1 to ensure personal data of the electors in question was protected from unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP 4(1) concerning the security of personal data.**

Investigation Case (2) – The REO wrongly attached a reply slip submitted by an Election Committee member to a test email

Background

35. On 28 April 2022, the REO submitted another data breach notification to the PCPD, reporting that a staff member wrongly attached a reply slip (the Reply Slip) containing the personal data of an Election Committee (the EC) member and his assistant to a test email which was sent to 38 EC members and 26 EC members' assistants (Incident 2). The Reply Slip contained the names, email addresses, contact numbers of the EC member and his assistant, and the signature of the EC member.

36. The REO reported Incident 2 to the Electoral Affairs Commission, the CMAB and the OGCIO on the same date.

37. Upon receipt of the above data breach notification, the Commissioner commenced an investigation against the REO on 6 May 2022 pursuant to section 38(b) of the Ordinance in relation to Incident 2 to ascertain whether the relevant act of the REO in Incident 2 is in contravention of the requirements under the Ordinance.

Information Obtained from the Investigation

38. During the course of the investigation, the Commissioner reviewed and considered the information provided by the REO in relation to Incident 2, including an internal investigation report provided by the REO, and a summary report published by the REO on 13 September 2022[10]. The Commissioner also considered the follow-up and remedial actions taken by the REO in the wake of Incident 2.

[10] https://www.reo.gov.hk/pdf/incident_report/Summary_Report_data_breach_incident_April2022(Eng).pdf

Background and Occurrence of Incident 2

39. The polling day of the 2022 Chief Executive Election (the Election) was held on 8 May 2022. To prepare for the Election, the REO issued a letter to all EC members on 25 March 2022 providing them with information relating to the Election and inviting them to provide their email addresses and mobile phone numbers and those of their assistants by completing and returning a reply slip by 6 April 2022 so as to facilitate the REO and other departments to promptly notify them by SMS or email of the latest electoral and contingency arrangements in relation to the Election on the polling day and when necessary.

40. On 22 April 2022, the REO issued another letter to EC members, reminding them in case of urgent needs or emergencies on the polling day (e.g. change of polling date or hours, implementation of contingency arrangements for polling or counting), the REO would notify the EC members of the latest electoral or contingency arrangements by SMS and/or email messages via the mobile phone numbers and/or email addresses provided by them. The REO also planned to issue test SMS and/or email messages on 27 April 2022 to EC members and/or their assistants who had provided their mobile phone numbers and/or email addresses to ensure that they could receive the relevant information.

41. An Electoral Officer (the Electoral Officer) was tasked with the sending of test SMS and/or emails, to be assisted by four Executive Assistants. Upon receipt of the reply slips provided by the EC members and their assistants, the information provided in the reply slips, which related to about 1,800 EC members and their assistants would be manually inputted onto a computer master list (the Master List). The information included the addresses, email addresses and mobile phone numbers of the EC members as well as the names, email addresses and mobile phone numbers of their

assistants. The Electoral Officer and the four Executive Assistants would conduct the checking.

42. Subsequently, the REO arranged a Senior Project Officer (the SPO) to oversee the task of issuing test emails (and SMS). Since the SPO spotted inaccuracies in the Master List despite multiple checkings on 27 April 2022 (the date when the REO planned to send the test emails), she instructed staff members to check the email addresses and issue the test emails in batches. On the other hand, as most of the reply slips were returned through email and it would be time-consuming and wasteful to print them, relevant staff conducted checking with the electronic copies of the reply slips directly.

43. The test emails were drafted by two Executive Assistants and went through the following checking steps before they were sent out from the Executive Assistants' computers:

	Responsible Staff	**Checking Steps Required**
First Checking	Executive Assistants	To cross-check the email addresses of recipients inputted in the 'bcc' fields of the draft test emails against the email addresses provided in the reply slips returned by EC members and/or their assistants to ensure that the email addresses were identical
Second Checking	The Electoral Officer	To check the content of the draft test emails and cross-check whether the email addresses entered into the draft test emails were consistent with the

		email addresses provided in the reply slips returned by EC members and/or their assistants to ensure that the email addresses were identical
Third Checking	The SPO	To cross-check the content of the draft test emails and the email addresses entered into the draft test emails were consistent with the email addresses provided in the reply slips returned by EC members and/or their assistants to ensure that the email addresses were identical

44. To facilitate checking, the Executive Assistants responsible for issuing the test emails would split their computer screens into two halves, with the left-hand side showing the draft test emails and the right-hand side showing the electronic copies of the reply slips. The Executive Assistants would use the up and down arrow keys on the keyboard to select the corresponding reply slips (shown in a preview window) and check against the email addresses inputted into the 'bcc' fields of the draft test emails one-by-one. Thereafter, the Electoral Officer and the SPO would conduct the second and third checking using the Executive Assistants' computers respectively. The Executive Assistants would only issue the relevant emails by pressing the "Send" button after the SPO had cross-checked the email addresses with the electronic copies of the reply slips and confirmed the contents of the test emails to be accurate.

45. The REO started issuing test emails in batches at 1:37 a.m. on 28 April 2022. To speed up the process, the SPO instructed that the second

checking be removed starting from the fourth batch of test emails so that the Electoral Officer could assist in drafting test emails.

46. As at 6:02 a.m. of 28 April 2022, the REO had issued 13 batches of test emails to 848 EC members and their assistants. At the same time, the Electoral Officer discovered in the course of reviewing the issued test emails that an email sent to 38 EC members and 26 assistants at 4:42 a.m. had the Reply Slip wrongly attached to it. Subsequently, the responsible staff members switched to reviewing the email addresses concerned and confirming the test emails using hard copies of the reply slips, and finished sending out the remaining 18 batches of test emails on 29 April 2022.

Personal Data Affected

47. Incident 2 concerned the names, email addresses and phone numbers of an EC member and his assistant, and the signature of the EC member.

REO's Investigation Findings

48. The REO's investigation report indicated that according to the workflow of preparing and checking the draft test emails, it was believed that staff wrongly attached the Reply Slip to one of the test emails, thereby leading to Incident 2. The REO was not able to ascertain the actual process of occurrence of the incident, but considered the following two scenarios to be the possible causes: -

(1) An Executive Assistant (purposedly or accidentally) attached the Reply Slip to the test email when preparing the draft test email; or
(2) The SPO (purposedly or accidentally) attached the Reply Slip to the test email when she conducted the checking.

49. The REO believed that the work process of manually inputting the information on the reply slips was prone to human errors, and that the way the staff checked the email addresses might have caused electronic copies of the reply slips to be attached to test emails accidentally. Besides, the staff did not double-check whether the test emails contained any inappropriate attachments before issuance.

REO's Follow-up Actions and Improvement Measures

50. Upon discovery of Incident 2, the REO had immediately changed the checking procedures by cross-checking the email addresses of the remaining batches of test emails using hard copies of the reply slips to avoid wrongly attaching electronic copies of reply slips to the test emails.

51. On 28 April 2022, the REO informed the EC members and/or their assistants who received the Reply Slip and requested them to delete the Reply Slip immediately and permanently, and informed the affected EC member and his assistant of the incident with apology.

52. To further enhance information security and prevent the reoccurrence of similar incidents, the REO has undertaken to review the workflow of handling personal data from time to time and make necessary enhancements, as well as to forestall any work procedures which are prone to mishandling of personal data. At the same time, the REO has undertaken to explore the feasibility of making use of information technology to collect personal data from EC members and issue emails in bulk with a view to preventing human errors.

Findings and Contravention

The REO as the data user in Incident 2

53. Similar to Incident 1, the REO is the data user in Incident 2 under section 2(1) of the Ordinance, and was required to comply with the requirements of the Ordinance, including the six DPPs set out in Schedule 1 to the Ordinance.

Data Protection Principle 4(1)

54. As stated above, pursuant to DPP4(1) in Schedule 1 of the Ordinance, a data user is obliged to take all practicable steps to ensure that the personal data held by it is protected against unauthorised or accidental access, processing, erasure, loss or use.

55. Having considered the facts of Incident 2 and the evidence obtained during the course of investigation, the Commissioner considers that the following reasons had led to the occurrence of Incident 2: -

(1) Staff negligence and inadequate awareness of data protection

56. According to the REO's investigation report, it is believed that staff inadvertently attached the Reply Slip to one of the test emails, thus resulting in the occurrence of Incident 2. The REO considered the following two scenarios to be the possible causes: the Executive Assistant purposedly or accidentally attached the Reply Slip to the test email when preparing the draft test email; or the SPO purposedly or accidentally attached the Reply Slip to the test email when she conducted the checking. Apparently, if the relevant staff involved had been more cautious in compiling the Master List and checking the draft test emails, Incident 2 could have been avoided. As a matter of fact, if the test email with the

Reply Slip wrongly attached had gone through the first and third checking, relevant staff members should have been able to spot the mistake during these two tiers of checking. The occurrence of Incident 2 clearly reflected the lack of awareness to personal data protection and lack of vigilance in ensuring the accuracy of personal data on the part of the staff members involved.

(2) Deficiencies in the work process of the REO

57. According to the workflow of the REO, the personal data of the EC members and their assistants contained in the reply slips related to Incident 2 were manually entered into the Master List without any systematic checking arrangements. The SPO only received the Master List for the first time on the date of the scheduled issuance of the test emails (i.e. 27 April 2022) and discovered then that the information contained therein was inaccurate.

58. The failure to ensure accuracy of the Master List resulted in last-minute crossing-checking of email addresses in draft test emails against the reply slips at abnormal working hours (the Commissioner noted that the email with the Reply Slip enclosed was sent at 4:42 a.m. of 28 April 2022). This overtime work apparently caused fatigue on the staff involved and increased the risks of human errors. Had the REO conducted proper checking and ensured the accuracy of the Master List before 27 April 2022, there would be no need to retrieve the electronic copies of the reply slips for last-minute checking, and Incident 2 would not have occurred.

59. As regards the mode of checking the draft test emails, it was noted that in order to facilitate checking, the computer screens of the Executive Assistants were split into two halves, with the left side displaying the draft test emails while the right side displaying the electronic copies of the reply

slips. The Executive Assistants used the up and down arrow keys on the keyboard to select the corresponding reply slips (to be shown in the preview window) to cross-check with the email addresses in the 'bcc' fields in the draft test emails one-by-one. Apparently, the said mode of checking was the main cause of the accidental dragging of the Reply Slip to the test email concerned by staff. Such arrangement, which appears to be adopted for work convenience and on an ad hoc basis, showed a failure on the part of the REO to incorporate privacy protection into work procedures and make adequate assessment on the impact on personal data privacy.

60. As a matter of fact, the second checking was at some stage removed by the SPO in order to release the Electoral Officer to help draft test emails and speed up the whole process. This significantly impaired the effectiveness of the 3-tier checking mechanism and was one of the contributing factors to the incident.

(3) Absence of written procedures for the relevant work

61. There were no written procedures on the mechanisms for sending the test emails, including the steps described in paragraphs 43 to 44 above. Reliance was placed on communication among relevant staff in the workflow involved. The lack of written procedures setting out clearly the checks required before sending the test emails naturally increases the risks of human deviations and non-compliances with the necessary steps, thereby undermining the relevant safeguards for the protection of personal data.

Conclusion: REO contravened DPP4(1)

62. Having considered all relevant evidence in this case, **the Commissioner considers that Incident 2 was mainly caused by human errors. It stemmed from the negligence and lack of awareness of data protection on the part of the relevant staff and deficiencies in the REO's relevant workflow. In the case of Incident 2, the inaccuracies of the Master List apparently led to a sudden change in the workflow and last-minute cross-checking of email addresses in draft test emails against the reply slips by staff well after mid-night. The Commissioner considers that if the REO had proper workflow in place to ensure the Master list was promptly and accurately prepared, the staff members involved would not have to conduct last-minute manual checking under tight time constraints or use unreliable method to conduct the checking. Meanwhile, if the staff members involved had been more cautious in the checking process, Incident 2 could have been avoided.**

63. **In addition, the REO did not have any written procedures in relation to the mechanism of sending test emails, thus increasing the risks of human errors and non-compliance with the necessary steps. The Commissioner understands that staff of the REO were working under huge pressure in conducting last-minute checks. However, the lack of written procedures inevitably increased the risks of human errors, especially when the staff concerned needed to work for prolonged hours and the removal of the second checking to expedite the whole process undermined the effectiveness of the original three-tier checking mechanism.**

64. **Based on the above, the Commissioner considers that the REO had not taken all practicable steps to ensure that the personal data of EC members and their assistants held by it was protected from**

unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP4(1) concerning the security of personal data.

Enforcement Action

65. Section 50(1) of the Ordinance provides that following the completion of an of an investigation, if the Commissioner is of the opinion that the relevant data user is contravening or has contravened a requirement under the Ordinance, the 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.

Incident 1

66. Having found that the REO contravened DPP4(1) of Schedule 1 to the Ordinance in Incident 1, the Commissioner exercised her power pursuant to section 50(1) of the Ordinance to serve an Enforcement Notice on the REO directing it to take the following steps to remedy the situation and prevent recurrence of the contravention:

(1) Implement technological security measures to restrict unauthorised employees from using any email system of the REO to send emails or files containing personal data to email accounts that do not belong to the REO;

(2) Strengthen training in respect of information security and the protection of personal data, including:

(i) Organise talks/seminars/workshops on information security and the protection of personal data for all staff members at least twice a year;

(ii) Offer talks/seminars/workshops on information security and the protection of personal data to all newly joined staff, and

establish an assessment mechanism to ensure the understanding of the relevant course content; and

(iii) Establish a mechanism for staff members to review the course content on information security and the protection of personal data on an annual basis;

(3) Record the progress of training as mentioned in item (2) above, and review and assess the participation and effectiveness of the relevant training plan annually to ensure the effectiveness of the relevant training and that it includes the latest information; and

(4) Provide documentary proof to the Commissioner within two months from the date of the Enforcement Notice, showing the implementation of items (1) to (3) above.

Incident 2

67. Having found that the REO contravened DPP 4(1) of Schedule 1 to the Ordinance in Incident 2, the Commissioner exercised her power pursuant to section 50(1) of the Ordinance to serve an Enforcement Notice on the REO directing it to take the following steps to remedy the situation and prevent recurrence of the contravention:

(1) Review and improve the workflow of collecting personal data from EC members and issuing bulk emails which contain personal data;

(2) Based on the review result of (1) above, devise/review relevant written operational procedures/guidelines, including the procedures of issuing test emails to EC members and relevant parties (if the REO would still issue test emails in the future);

(3) Strengthen training in respect of information security and the protection of personal data, including:

(i) Organise talks/seminars/workshops on information security and the protection of personal data for all staff members at least twice a year;

(ii) Offer talks/seminars/workshops on information security and the protection of personal data to all newly joined staff, and establish an assessment mechanism to ensure the understanding of the relevant course content; and

(iii) Establish a mechanism for staff members to review the course content on information security and the protection of personal data on an annual basis;

(4) Record the progress of training as mentioned in item (3) above, and review and assess the participation and effectiveness of the relevant training plan annually to ensure the effectiveness of the relevant training and that it includes the latest information; and

(5) Provide documentary proof to the Commissioner within two months from the date of the Enforcement Notice, showing the implementation of items (1) to (4) above.

68. Under section 50A of the Ordinance, a data user who contravenes an enforcement notice commits an offence and is liable to a maximum fine at level 5 (i.e. HK$50,000) and imprisonment for 2 years on a first conviction.

69. As mentioned above, the Commissioner considers that both data breach incidents involved human negligence. The Commissioner noticed that the REO is taking follow-up actions against the staff members concerned

under the existing civil service disciplinary mechanism. As the scope of the investigations is to determine whether the REO had taken all practicable steps to protect personal data held by it pursuant to DPP4(1) in the incidents concerned, the disciplinary actions taken by the REO against individual staff members fall outside the ambit of this report.

70. Although there is room for improvement in the REO's training regarding information security and the protection of personal data, as well as the REO's information security measures, the Commissioner is pleased to note that the REO promptly submitted data breach notifications after both data breach incidents, was cooperative throughout the course of the PCPD's investigation, and made efforts to learn from the incidents. The Commissioner notes that the REO has already enhanced security measures and reviewed the relevant workflow of personal data handling to strengthen the protection of personal data privacy.

Recommendations

71. Section 48(2) of the Ordinance provides that the Commissioner may, after completing an investigation and if she is of the opinion that it is in the public interest to do so, publish a report setting out the result of the investigation and any recommendations and such other comments arising from the investigation that the Commissioner thinks fit to make. Apart from serving enforcement notices to the REO pursuant to section 50(1) of the Ordinance in relation to the two data breach incidents, the Commissioner wishes to make the following recommendations to organisations which possesses a huge amount of personal data through this Report.

Thoroughly Implement a Personal Data Privacy Management Programme

72. Data users, especially organisations in possession of a large amount of personal data, should implement the Personal Data Privacy Management Programme (PMP) to embrace personal data privacy protection as part of their data governance. A PMP could assist organisations in effectively managing the whole lifecycle of personal data from collection to disposal, allow organisations to handle data breach incidents promptly, and ensure compliance with the Ordinance.

Conduct Privacy Risk Assessments and Formulate Specific Guidelines for Non-Routine Work

73. Data users should conduct privacy risk assessments for non-routine work arrangements (e.g. work-from-home arrangements, or procedures that involve the handling of a large amount of personal data) to assess the risks on data security and areas of personal data privacy. Based on the results of risk assessment, organisations should review their existing policies and

practices, make necessary adjustments or consider formulating specific guidelines for employees to follow.

Devise Effective Education and Training Plans

74. Data users, especially organisations that hold a large amount of personal data, should educate their staff on the importance of respecting and protecting the personal data privacy and complying with the requirements of the Ordinance. In this regard, organisations should establish appropriate education and training plans to effectively and continuously communicate personal data security policies, procedures and practical guidelines to all employees to ensure that they know and understand the relevant policies and requirements, and provide clear means for staff to access the relevant information promptly. In addition, organisations should also take measures to regularly review the effectiveness of the relevant plans.

Deploy Information Security Measures to Mitigate the Risk of Human Errors

75. Organisations that handle a large amount of personal data should consider adopting technology extensively to mitigate the risks of human errors. In terms of daily processing of personal data, organisations may consider using automated means or deploying appropriate systems to collect, process and compare personal data to increase the accuracy of data; in terms of data security, organisations should deploy proper technological measures to effectively protect personal data held by them and monitor the use of information equipment (including email systems) by employees monitored, so as to avoid data breach incidents.

— End —