Data Breach Incident of the Registration and Electoral Office on 28 April 2022

Summary Investigation Report

A data breach incident occurred on 28 April 2022 in which a staff member of the Registration and Electoral Office ("REO") wrongly attached a reply slip (with personal data) provided by an Election Committee ("EC") member in a test email issued to 64 EC members or their assistants.

2. This report provides an account of the incident and the findings of the investigation of the incident conducted by the REO; the follow-up actions taken by the REO and related parties thus far; and improvement measures that have been/will be taken by the REO to forestall the recurrence of similar incidents in future.

Background

3. The polling day of the 2022 Chief Executive ("CE") Election fell on 8 May 2022. The REO issued a letter to all EC members on 25 March 2022 providing them with information relating to nomination in the 2022 CE Election and other electoral arrangements. In the letter, EC members were also requested to provide to REO their email addresses and mobile phone numbers as well as those of their assistants by completing and returning a reply slip by 6 April 2022 so as to facilitate REO and other departments to inform them immediately by SMS or email of the most updated electoral and contingency arrangements on the polling day of the 2022 CE Election and as needs arose. On 22 April 2022, REO issued another letter to all EC members advising them that in case of urgent needs or emergencies on the polling day (e.g. change of polling date or hours, implementation of contingency arrangements regarding polling and counting, etc.), REO would inform them of the latest electoral arrangements or contingency measures by SMS and/or email message via the mobile phone numbers and/or email addresses provided by them earlier. REO would issue the test SMS and/or email messages to EC members and/or their assistants who had provided their mobile phone numbers and/or email addresses on 27 April 2022.

4. Upon receipt of the reply slips provided by the EC members and their assistants, the REO inputted the information on the reply slips involving about 1,800 persons into a master list one by one manually. Before issuance of test emails, staff of the REO would cross-check the information on the master list with that on the reply slips to ensure that the test emails would correctly be issued to the EC members or their assistants.

5. Staff of the REO responsible for issuing the test emails conducted the checking work on 27 April 2022. Considering that it would easily make mistakes for checking over 1,800 email addresses in one go, the staff then checked the email addresses and issued the test emails by batches. Besides, as many reply slips were returned by email, it would take time to print them out and cause waste. The staff thus directly used the soft copy each of the reply slips to conduct checking.

6. When conducting the checking, the staff member responsible for drafting the test emails would input the email addresses of the recipients of a batch in the bcc field of the draft email, and would check the email addresses inputted in the bcc field of the draft test email one by one against the soft copy each of the reply slips received from EC members on the computer. Another staff member would cross-check the email addresses against the soft copy of the reply slips again and confirm the accuracy of the content of the test email before the test email was issued.

The Incident

7. In the early morning of 28 April 2022, REO issued a total of 13 batches of test emails to 848 EC members and their assistants. In the morning of the same day, a staff member of REO discovered that a soft copy of the reply slip returned by an EC member to REO in early April 2022 was wrongly attached in a test email issued to 64 EC members or their assistants in the early morning of 28 April 2022. The personal data involves the names, email addresses and mobile phone numbers of the concerned EC member and his assistant, as well as the signature of the EC member.

Immediate Follow-up Actions Taken by REO

8. Upon notification of the incident on 28 April 2022, the REO

immediately took the following follow-up actions on the same day -

(a) reported to the Electoral Affairs Commission, the Constitutional and Mainland Affairs Bureau ("CMAB"), the Privacy Commissioner for Personal Data ("PCPD") and the Office of the Government Chief Information Officer ("OGCIO");

(b) informed the EC members or their assistants who received the test email containing the attachment and appealed for their assistance to delete the attachment immediately and permanently; and informed the affected EC member and his assistant of the incident and to express sincere apologies;

(c) confirmed that other batches of test emails did not have similar mistake; and

(d) the staff member involved had been deployed away from his existing duty, and would not be assigned with duties involving the handling of personal data and would be investigated.

9. According to the findings of the investigation conducted on the date of the incident, REO suspected that the soft copy of the reply slip of the EC member concerned had been accidentally attached by staff to the test email issued to the EC members or their assistants during the work process. To prevent the recurrence of similar incident, following the incident, REO had immediately improved the procedures for checking and issuing the remaining batches of test emails, and instructed staff to cross-check the email addresses inputted in the bcc field of the draft test emails by using the hard copy of both the reply slips and the draft test emails, instead of viewing the soft copy of the reply slips on the computer (as the subject team did before the incident) to avoid it being dragged to the email accidentally during the work process. The staff member of REO who was responsible for the final check had to confirm the accuracy of both the email addresses and content of the test emails before they were issued. The REO staff followed the instructions to check the test emails. All the remaining 18 batches of test emails to a total of 963 EC members and their assistants were issued on 28 and 29 April 2022.

REO's Investigation and Findings

10. REO had completed the investigation of the incident. In light of the findings of the investigation of the incident, the REO believed that the soft copy of the reply slip concerned had been accidentally attached by staff to the test email issued to the EC members or their assistants during the work process which caused the incident. Investigation revealed the following inadequacies in the issuance of test emails -

(a) The contact information provided by the EC members in the reply slips was inputted manually in the computer. It will prone to human errors during the work process.

(b) As stated in paragraph 5 above, to reduce waste and to increase efficiency in checking, the staff used the soft copy (instead of hard copy) of the reply slips provided by the EC members earlier to conduct checking on the computer. Such checking arrangement might cause the soft copy of the reply slip being dragged to the test email accidentally.

(c) The staff did not double-check that the test email had not contained any inappropriate attachments before it was issued.

Improvement Measures to be Taken by REO

11. In view of the inadequacies mentioned above, the REO will review the workflow of handling personal data from time to time and make necessary enhancements to ensure that all procedures comply with the prevailing legislation, regulations and guidelines, as well as to forestall any work procedures which are prone to mishandling of personal data. The REO will also explore the feasibility of making use of information technology to collate personal data from EC members and to issue emails in bulk with a view to preventing human errors. The REO will also take follow-up action on the performance of the staff concerned as reflected in this incident.

Special Information Security Review by OGCIO

12. In view of a data breach incident reported by the REO in March

2022[1], a working group comprising representatives from the OGCIO, CMAB and REO has already been formed to conduct a special review on information security of the REO. The review adopts a risk-based approach and makes reference to industry best practices to review the REO's current information security management practices so as to identify potential improvement opportunities for strengthening the information security safeguard of the REO and developing a positive information security culture so as to enhance the security posture and cyber resilience of the REO. The REO will prioritise the implementation of these recommendations and bid for the required financial and staffing resources.

Investigation by PCPD

13. The PCPD is carrying out an investigation against the REO under section 38(b)(ii) of the Personal Data (Privacy) Ordinance ("PD(P)O") (Cap. 486) to ascertain whether the relevant act and/or practice of the REO in handling and protecting the personal data of EC members and their assistants at the material time of the incident is in contravention of the requirements under the PD(P)O. PCPD's investigation is underway. Besides, the PCPD is conducting an inspection of the personal data system of the REO.

Registration and Electoral Office
September 2022

[1] The data breach incident occurred on 23 March 2022 in which a staff member of the REO did not follow the departmental guidelines and sent files containing 15,070 electors' particulars to her personal email address to facilitate her work. However, she entered an incorrect email address, resulting in the files being sent to an unknown recipient.