Data Breach Incident of the Registration and Electoral Office on 23 March 2022

Summary Investigation Report

A data breach incident occurred on 23 March 2022 in which a staff member of the Registration and Electoral Office ("REO") did not follow the departmental guidelines, intending to send files containing 15,070 electors' particulars to her personal email address to facilitate her work. However, the staff member entered an incorrect email address, resulting in the files being sent to an unknown recipient.

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. One of the main duties of the staff member who wrongly sent files containing electors' particulars to an unknown recipient by email is to lead her team to conduct data matching exercises with other Government departments, including the subject case for which the tenancy agreements of the electors in the public housing estates have been terminated as provided by the Housing Department ("HD"). Upon receipt of the information from HD, the REO has to compare the electors' residential addresses kept by the REO with those provided by the HD. If the address of an individual elector is identical, REO would have a reasonable doubt that the elector's registered residential address is no longer his/her only or principal residential address, and he/she will be subject to the inquiry procedures under section 7 of the Electoral Affairs Commission (Registration of Electors) (Legislative Council Geographical Constituencies) (District Council Constituencies) Regulation (Cap. 541A). If the addresses between HD's record and REO's record for an individual elector are different, REO would reasonably believe that the residential address has been updated and would take no further action.

The Incident

4. At 7:03pm on 23 March 2022, the staff member concerned intended to issue an email attaching two Excel files to her personal email account to facilitate her work, but she entered an incorrect email address, resulting in the files being sent to an unknown recipient. The aforesaid two Excel files contained particulars of 15,070 electors[1] (5,264 and 9,806 electors' particulars were contained in these two files), including their names and residential addresses in the public housing units for which their tenancy agreements had been terminated as provided by the HD. In addition, the two files also contained the names and registered residential addresses of these electors in the REO's record. Apart from the Chinese and English names as well as residential addresses of the electors, there is no other personal data such as identity card numbers, dates of birth and gender. The staff member concerned realized that she had mistakenly sent the email to another email address after some 10 minutes as she noticed that the email did not reach her personal email account.

Immediate Follow-up Actions Taken by REO

5. Upon notification of the incident by the staff member on 24 March 2022, the REO requested the unknown recipient via an email on the same day to permanently and immediately delete the relevant files and contact the REO for follow-up. The REO reported the incident to the Electoral Affairs Commission, the Constitutional and Mainland Affairs Bureau ("CMAB") and the Office of the Government Chief Information Officer ("OGCIO"). The REO also reported the incident to the Police for investigation and filed the data breach incident to the Privacy Commissioner for Personal Data ("PCPD") on the same day.

6. The REO issued a press release on 25 March 2022 giving the public an account of the incident. For the affected electors, the REO informed them in writing of the incident.

[1] In accordance with section 2 of the Personal Data (Privacy) Ordinance (Cap. 486), personal data means, inter alia, any data relating directly or indirectly to a living individual and data subject, in relation to personal data, means the individual who is the subject of the data. Hence, excluding the 103 deceased electors, the total number of the affected data subjects is 14,967.

Investigation by Police

7. Upon receipt of REO's report of the incident, the Police conducted an investigation into the case. The Police had later successfully contacted the recipient of the concerned email. Police investigation confirmed that the recipient did not open the concerned email with files containing electors' particulars and had already deleted the email. After investigation and examination of evidence gathered, the Police confirmed that the evidence gathered was insufficient to support a charge against any person. No prosecution action would thus be taken by the Police.

REO's Investigation and Findings

8. The REO completed the investigation of the incident. It was found that the staff member concerned indeed sent two more emails enclosing official documents which contained electors' particulars to her personal email accounts successfully on 23 March 2022. The first one was sent at 5:43pm containing names of around 1,000 electors (with their English and Chinese names together with some internal reference numbers which could not be used for identifying an individual). The second one was sent at 7:58pm containing the same files attached in the email in question (i.e. the one wrongly sent to the unknown recipient at 7:03pm). Despite knowing that the last email had been wrongly sent to an unknown recipient, the staff without thorough consideration, sent the files to her personal email account again. The staff concerned confirmed that the above documents had been deleted from her personal email accounts.

9. REO's investigation revealed that the staff member concerned did not follow the guideline set out in the relevant departmental circular 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***".

10. The staff member concerned is considered to have committed misconduct of negligence in handling personal data and contravening departmental guidelines on information technology security by sending the three emails containing official documents to her personal email accounts, i.e. the email at 5:43pm containing names of around 1,000 electors and the two

emails with personal data of 14,967 electors at 7:03pm and 7:58pm respectively on 23 March 2022, with the second email sent to an unknown recipient because of entering an incorrect email address. She had admitted that her act of sending files containing personal data of electors was wrong and was remorseful for her wrongdoings. The REO is taking follow-up action against the staff member concerned under the existing civil service disciplinary mechanism.

Improvement Measures Taken by REO

11. To further enhance data security and to forestall the recurrence of similar incidents of using personal email accounts for discharging official duties or for transmitting classified information or personal data, technological restrictions have been imposed on staff in the relevant division of REO other than those who have genuine operational need, so that their official email accounts cannot send out emails to internet email addresses and their desktop computers cannot access the websites of the internet email service providers commonly used in Hong Kong (e.g. gmail, yahoo mail, Outlook, AOL mail, iCloud mail, etc.) with effect from early April 2022.

Special Information Security Review by OGCIO

12. A working group comprising representatives from the OGCIO, CMAB and REO has conducted 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 electors 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