Data Breach Incident of the Electrical and Mechanical Services Department
Investigation Findings

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

Background

The Office of the Privacy Commissioner for Personal Data (PCPD) completed its investigation in relation to a data breach incident reported by the Electrical and Mechanical Services Department (EMSD).

The investigation arose from a data breach notification submitted by the EMSD to the PCPD on 1 May 2024, reporting its suspicion that the personal data of members of the public in its possession was leaked. The data breach involved the personal data of persons who had undergone testing in the "restriction-testing declaration" (RTD) operations conducted in 2022 (the Incident).

The EMSD conducted a total of 14 RTD operations between March and July 2022 to carry out COVID-19 tests for the residents or visitors in 14 buildings (see Annex 1). To collect the data of persons who were subject to testing in the RTD operations, the EMSD procured and used the services of an e-Form Platform (the e-Form Platform) associated with the cloud platform ArcGIS Online and created 14 e-forms. The relevant e-forms and data were stored in the data repository of ArcGIS Online.

In late 2022, when the EMSD noted that the RTD operations had come to an end, it immediately notified the contractor not to renew the service contract after its expiry in late February 2023. According to the EMSD, the EMSD considered that the e-Form Platform account would be invalidated upon expiry of the contract, and the relevant information would be automatically deleted by the contractor. It was not until its receipt of the PCPD's notification on 30 April 2024 that the EMSD learned that the personal data of persons who had undergone testing in the RTD operations could be browsed by anyone at the relevant website of ArcGIS Online without logging into any account or password. The EMSD hence immediately requested the contractor to remove the personal data involved from the e-Form Platform on the same day, so that the public could no longer browse the relevant information. The EMSD also submitted a data breach notification to the PCPD on the next day.

The Incident affected the personal data of over 17,000 persons. The personal data involved included names, addresses, Hong Kong Identity Card (HKID card) numbers, telephone numbers, ages, genders, whether the persons were vaccinated, whether they were tested positive in PCR tests and the respective dates.

Based on the information provided by the EMSD, subsequent to the Incident, the EMSD has strived to learn from the Incident and has implemented a series of measures and initiatives, which included strengthening privacy management, comprehensively reviewing the work and guidelines on the handling of personal data, stepping up staff training and supervision of contractors and enhancing departmental information technology support systems, so as to establish a more robust privacy protection framework and a corporate culture that values the protection of personal data.

Investigation Findings

In the course of the investigation, the PCPD has conducted five rounds of enquiries with the EMSD and approached the contractor twice to obtain relevant information. The PCPD thanked the EMSD and the contractor for their cooperation and the provision of the information and documents requested in the investigation. **Having considered the circumstances of the Incident and the information obtained during the investigation, the Privacy Commissioner for Personal Data (Privacy Commissioner), Ms Ada CHUNG Lai-ling, found that the following deficiencies of the EMSD were the main contributing factors of the occurrence of the Incident:-**

> **1. Lack of written policies on the retention of personal data collected in the RTD operations**. Hence, there was no clear guidance on the storage and disposal of data. While the EMSD might not be able to specify the retention period or formulate a data retention policy before or during the RTD operations, nonetheless all along it had only relied on the notification given to the contractor in late 2022 not to renew the contract as the basis for suggesting that a data retention period had actually been specified. However, there had not been any written policy specifying the retention period of the aforesaid data. Such written policies could provide a clear basis for the retention and disposal of data and could play an important role in this regard.
>
> In particular, for this case, the data involved sensitive personal data, including the persons' names, ages, genders, full addresses, phone numbers, as well as their HKID card numbers and PCR test results. Besides, the Incident affected over 17,000 persons. Therefore, the EMSD should be particularly vigilant and cautious in handling the data involved.

2. Failure to make unequivocal request to the contractor for deletion of the relevant data in late 2022, when the EMSD became aware that the RTD operations had come to an end. In notifying the contractor not to renew the contract, the EMSD had not explicitly requested the contractor to delete the personal data involved in the Incident. In fact, it was only when the EMSD became aware of the Incident on 30 April 2024 that it requested the contractor to remove the personal data involved from the e-Form Platform on the same day. The relevant data was then removed that evening, so that they could no longer be accessed by the public. It is evident that the data would be removed upon a request made with the contractor.

The Privacy Commissioner considered that requesting the contractor to delete the relevant data when the EMSD notified the contractor not to renew the contract would have been an effective and practicable step to safeguard the personal data involved. However, the EMSD did not take this action.

3. Failure to take the initiative to delete the personal data involved, particularly during the period from late December 2022 to late February 2023 when the EMSD was still able to log in to the e-Form Platform to manage the personal data stored therein. Instead, the EMSD only waited for the contract with the contractor to expire, without taking the initiative to check and delete the personal data from the platform to avoid unnecessary or excessive retention of the personal data. This is a clear deficiency; and

4. Failure to properly follow up with the contractor on the deletion of data as the EMSD merely assumed that the contractor would act on its own volition after the expiry of the contract. The EMSD had never urged, checked or reminded the contractor to delete the personal data from the e-Form Platform, and had never sought to understand or monitor the progress or effectiveness of the contractor's relevant actions. The EMSD, as the data user, should not merely await passively for the contractor to take action, nor should it ride on its trust in the contractor and not to verify the work done by the contractor. This is another obvious deficiency.

The Privacy Commissioner's Decision

The Privacy Commissioner, Ms Ada CHUNG Lai-ling, understood that amid the severe epidemic situation, departments involved in the RTD operations needed to deploy resources and act quickly. Owing to the time constraints, the EMSD might not have considered the policies and arrangements for deletion of personal data when they planned and conducted the

RTD operations. However, since then, the EMSD has not formulated a policy on the retention period of the relevant personal data, nor has it made an unequivocal request to the contractor for data deletion; the EMSD also failed to proactively delete the personal data, or to follow up on and check the deletion of personal data by the contractor after the completion of the RTD operations, which resulted in the unnecessary exposure of the relevant personal data to the risk of data leakage. It is clear that not only had the EMSD failed to comply with the requirements of the Personal Data (Privacy) Ordinance (PDPO), it had also fallen short of the reasonable expectations of the public. In the circumstances, the Privacy Commissioner found that the EMSD:

(i) had not taken all practicable steps to ensure that the personal data involved was not kept longer than was necessary for the fulfilment of the purpose for which the data was used, thereby contravening Data Protection Principle (DPP) 2(2) of the PDPO concerning the retention of personal data; and

(ii) had not taken all practicable steps to ensure that the personal data involved was protected against unauthorised or accidental access, processing, erasure, loss or use, thereby contravening DPP4(1) of the PDPO concerning the security of personal data.

The Privacy Commissioner has served an Enforcement Notice on the EMSD, directing it to take measures to remedy the contraventions and prevent recurrence of similar contraventions in future.

Ada CHUNG Lai-ling
Privacy Commissioner for Personal Data
9 December 2024

Annex 1

Dates, buildings and number of persons involved in the 14 RTD operations

Dates of operations	Building	Number of persons involved
3-4 / 3 / 2022	Tak Ying House, Tak Long Estate	1,506
6-7 / 3 / 2022	Yan Ching House, Kai Ching Estate	1,451
9-10 / 3 / 2022	Oi Ming House, Yau Oi Estate	1,608
14-15 / 3 / 2022	Fu Leung House, Fu Cheong Estate	210
17-18 / 3 / 2022	Wu Fai House, Wu King Estate	1,330
19-20 / 3 / 2022	Tip Ying House, Butterfly Estate	1,348
21-22 / 3 / 2022	Sin Tat House, On Tat Estate	1,966
23-24 / 3 / 2022	Wai Tung House, Tung Tau (II) Estate	285
25-26 / 3 / 2022	Kwong Wai House, Kwong Fuk Estate	1,010
30/3 - 1/4/2022	Pok Yat House, Pok Hong Estate	1,823
12-13 / 4 / 2022	Cheung Fung House, Cheung Wah Estate	939
3-4 / 5 / 2022	Ming Toa House, Ming Tak Estate	1,582
30-31 / 5 / 2022	Un Shing House, Un Chau Estate	469
4-5 / 7 / 2022	Toi Fung House, Fung Tak Estate	1,798
	Total	**17,325**