Investigation Report

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

Security Measures Taken by Restaurants to Protect Customers’ Information Collected during the Registration Required under the COVID-19 Anti-pandemic Measures

Date of Issue: 28 October 2021

Executive Summary

Background

In response to the COVID-19 pandemic, the Government imposed requirements under the Prevention and Control of Disease (Requirement and Directions) (Business and Premises) Regulation (Cap. 599F) on responsible persons of restaurants to ensure that customers either scan the venue QR code with the “LeaveHomeSafe” mobile app or register their names, contact numbers and dates and times of their visits, before entering the premises, and for restaurants to keep such written or electronic records for 31 days (the “Restaurant Entry Requirement”).

Since the implementation of the Restaurant Entry Requirement on 18 February 2021, the PCPD has received complaints about the failure of restaurants to properly handle the registration data of customers. Having received the complaints, the Privacy Commissioner for Personal Data (the “Privacy Commissioner”) launched investigations into 14 complaints pursuant to the powers conferred on her under section 38(a)(i) of the Personal Data (Privacy)
Ordinance (Cap. 486) (the “Ordinance”).

Findings and Contravention

The Privacy Commissioner found that the retention period set by those 14 restaurants for keeping the registration data of customers did not exceed 31 days. In other words, the restaurants kept the data in accordance with data retention period as specified in the Restaurant Entry Requirement, in such a way that the relevant personal data was not kept longer than necessary for the fulfilment of the original purpose. This practice is commendable, as it is in compliance with the requirements of Data Protection Principle (DPP) 2(2) under the Ordinance.

Meanwhile, the Privacy Commissioner also found that 11 restaurants (namely, Triple O’s in Pacific Place of Admiralty, Spicy and Sour Noodle at Portland Street of Mongkok, Zaks in D’Deck of Discovery Bay, The Grill Room in the L. Square of Causeway Bay, Corner Kitchen at Tso Kung Square of Tsuen Wan, Bond at Tung Lo Wan Road of Tai Hang, Carnival Seafood Restaurant in Leung King Plaza of Tuen Mun, American Seafood & Grill in Fortune City One of Shatin, TW Yummy at Nathan Road of Yaumatei, Beef Noodle Box at Kam Ping Street of North Point and Ming Kee Cheung Fun at San Hong Street in Sheung Shui) used common registration forms or books, 1 restaurant (TamJai Yunnan Mixian at Kwai Yi Road in Kwai Fong) did not set up any collection box for the forms, 1 restaurant (House of Canton Restaurant in Cityplaza) failed to cover the collection box at all times, and 1 restaurant (Gyuugoku at Tai Tsun Street in Tai Kok Tsui) used uncut sheets of paper as common forms. The above practices had exposed the registered personal data to unauthorized or accidental access or use, and contravened DPP 4(1) of the Ordinance as regards the security of personal data.

Although the 14 restaurants subsequently took remedial actions to prevent recurrence in future, the Privacy Commissioner has decided to issue Enforcement Notices to the restaurants in question to request them to implement appropriate and practicable measures to protect the registration data of customers and specify the steps to be taken by the restaurants for preventing
recurrence of the contravention. The measures included providing written policy and guidance to their staff, as well as circulating the guidance regularly and providing training to raise the awareness of their staff to the protection of personal data privacy.

Reminders and Suggestions

The Privacy Commissioner wishes to make the following reminders and suggestions through this report: -

(1) Regardless of the scale of business, mode of operation and availability of resources, all restaurants have responsibility to comply with the requirements of the Ordinance in the collection, holding, processing and use of personal data, including:

- collecting personal data of customers in a lawful and fair manner, to the extent that it is necessary, adequate but not excessive; restaurants should inform data subjects of the purpose(s) of data collection and the classes of persons to whom the data may be transferred (DPP1);
- destroying the personal data when the purpose(s) for which the data is used has/have been fulfilled (DPP2);
- except with the express and voluntary consent of the data subject, personal data shall not be used for a new purpose (DPP3); and
- taking all practicable steps to protect personal data against unauthorized or accidental access, processing, erasure, loss or use (DPP4).

(2) In addition to incorporating privacy protection in the workflow of data processing, restaurants must also provide appropriate training and guidance for their staff.

(3) Restaurants must adopt measures to provide clear guidelines for their staff on the process and purpose of customer registration, and ensure
the proper conduct of their staff, so as to avoid the collection and processing of personal data from being hampered by human negligence or error. An explanation of the need and purpose of data registration to customers can help minimize unnecessary misunderstanding.

(4) In response to anti-epidemic measures, restaurants need to raise the awareness of their staff to personal data privacy protection. By strengthening personal data privacy protection, restaurants would be able to enhance their goodwill, competitive edges, and potential business opportunities.

To protect personal data, members of the public should be mindful of the privacy risks inherent in providing personal data for different restaurants. This is particularly true for citizens who frequently dine at different restaurants, if they choose to register personal information rather than using the “LeaveHomeSafe” mobile app, which effectively means that they may need to provide personal data for different restaurants daily. This, when compared with storing visiting records in the “LeaveHomeSafe” app in their own mobile phones, actually carries greater privacy risks.