LCQ9: Compliance checks and compliance investigations conducted by Office of Privacy Commissioner for Personal Data

Following is a question by the Hon Lam Cheuk-ting and a written reply by the Secretary for Constitutional and Mainland Affairs, Mr Patrick Nip, in the Legislative Council today (January 23):

Question:

Cathay Pacific Airways Limited announced on October 24 last year a leakage of the personal data of more than nine million passengers. The Office of the Privacy Commissioner for Personal Data (PCPD) announced on the following day and on November 5 respectively that it would initiate a compliance check on the incident and a compliance investigation against the company. Besides, there are comments that the number of compliance investigations initiated and the number of investigation reports published by PCPD in recent years have decreased drastically when compared with those before then. In response, PCPD stated that in accordance with the relevant legislation, a compliance investigation report would only be published where the Privacy Commissioner for Personal Data (Privacy Commissioner) was of the opinion that it was in the public interest to do so. Upon the completion of significant compliance checks or compliance investigations, PCPD would issue press statements, and receive and respond to media enquiries, thereby achieving the same effect as publishing an investigation report without employing the practice of "naming and shaming" the party investigated. In this connection, will the Government inform this Council if it knows:

(1) the differences between a compliance check and a compliance investigation, including those in the areas of the relevant procedure and follow-up actions;

(2) the respective numbers and details (including the topics, the dates on which the reports were published (if any) and the follow-up actions taken) of the compliance checks and compliance investigations completed by the incumbent Privacy Commissioner and the preceding two Privacy Commissioners during their terms of office;

(3) whether PCPD has assessed if its refrainment from adopting the practice of naming the organisations that have breached the data protection principles has undermined the effect of making other organisations to stay vigilant that may be achieved by PCPD conducting checks or investigations; and

(4) the criteria adopted by the Privacy Commissioner for determining whether it is in the public interest to publish a certain compliance investigation report?

Reply:

President,

The Hong Kong Special Administrative Region Government is highly concerned about the data breach incident of Cathay Pacific Airways. Currently, the Office of the Privacy Commissioner for Personal Data (PCPD) has initiated a compliance investigation under Section 38 of the Personal Data (Privacy) Ordinance (PDPO) in the wake of the incident. After consulting the PCPD, reply to various parts of the question is as follows:

(1) The PCPD has developed a set of procedures for handling data breach incidents. Upon receiving notification on a data breach incident, the PCPD will commence a compliance check to find out the facts and ascertain causes of the data leakage, and to evaluate the effectiveness of the remedial actions taken or to be taken by the organisations concerned. The PCPD will also advise and assist the organisations concerned in taking timely remedial measures to protect the interests of those who were affected. Having regard to the result of the compliance check, if the Privacy Commissioner for Personal Data (Privacy Commissioner) has reasonable grounds to believe that there may be a contravention of the requirements under the PDPO, he will initiate a compliance investigation under Section 38 of the Ordinance. The Privacy Commissioner is empowered under the PDPO to summon relevant persons to furnish evidence, enter premises to inspect personal data systems and collect evidence, among others, for the conduct of compliance investigations. Depending on the result of the compliance investigation, the PCPD may issue an enforcement notice to the organisations concerned.

(2) The numbers of compliance checks conducted from 2005/06 onwards, as set out in Annex 1, are summarised as follows:

Year	Average number of cases of compliance check per year
2005/06 – 2009/10 (5 years)	100
2010/11 – 2014/15 (5 years)	180
2015/16 – 2018 (3 years and 9 months)	272

There are many different types of compliance check cases. Generally speaking, these cases mainly involve the collection, accuracy, retention, use, access to and security of data in industries such as finance, education, retail, government departments and public organisations.

The numbers of compliance investigations from 2005/06 onwards and the investigation reports published in the same period are set out at Annex 2 and Annex 3 respectively. A summary is given below:

Year	Average number of cases of compliance investigations per year
2005/06 – 2009/10 (5 years)	4.4
2010/11 – 2014/15 (5 years)	29.8
2015/16 – 2018 (3 years and 9 months)	22.4

(3) The recent trend of data breach incidents has shifted from mostly improper collection and use of data in the past to breach of data security, such as data leakage and hacker attacks. The former is more discernible in terms of the nature of and liability for data breach. To facilitate cooperation from the organisations concerned, the PCPD has, since 2016, ceased to adopt the "naming and shaming" practice under normal circumstances. By doing so, the PCPD has been able to understand the detailed facts as soon as possible and stands a better chance of ascertaining whether there are reasonable grounds for the Privacy Commissioner to be of the opinion that there exists a contravention under the PDPOã€€before a compliance investigation is initiated. It also enables the organisations concerned to take remedial measures for safeguarding data privacy of individuals concerned (customers and consumers) at the earliest possible time. As a regulatory body, the PCPD discharges its statutory duties through result-based approaches. Apart from enforcement and sanctions, the PCPD also provide organisations with guidance, practical assistance and support on compliance and good practices of data protection.

(4) According to Section 48(2) of the PDPO, the Privacy Commissioner may, after completing an investigation and if he is of the opinion that it is in the public interest, publish a report setting out the result of the investigation, any recommendations or other comments arising from the investigation as he thinks fit to make. Since there is no definition of "public interest" in the PDPO, the Privacy Commissioner will, having regard to individual circumstances and Section 48(2) of the PDPO, deliberate on whether to publish an investigation report on compliance investigation while considering judgments and guidelines on relevant cases. Factors for consideration include but are not limited to the following:

1. the nature and circumstances of the incident in question;
2. the severity of the incident in question, including the amount and nature of personal data involved, the number of people affected and the impact on them;
3. whether the incident in question is minor or technical in nature;
4. the degree of culpability of the offender concerned;
5. whether there is cooperation between the offender and the regulatory body and whether the offender has demonstrated remorse, made commitment, compensated the victim(s), etc.;
6. the likely final disposition of the incident in question;
7. whether a new problem is embodied in the incident;
8. whether publishing a report can achieve an educational purpose or a

deterrent effect or prevent the recurrence of similar incidents;

9. the availability and efficacy of alternatives to publishing a report, such as cautions, undertakings or other acceptable approaches for handling the incident;
10. information on the incident in question is available in the public domain and publishing a report allows the public to learn the truth or play a monitoring role; and
11. making public the report concerned is conducive to debate about a matter of common concern.

Apart from publishing a report on compliance investigation, the PCPD will also make public the result of completed compliance investigation through its annual report and/or media statements.