LCQ2: Prevention of personal data breaches and financial crimes

â€‹ Following is a question by the Hon Carmen Kan and a reply by the Secretary for Constitutional and Mainland Affairs, Mr Erick Tsang Kwok-wai, in the Legislative Council today (January 22):

Question:

Regarding prevention of personal data breaches and financial crimes, will the Government inform this Council:

(1) of the number of data breach incidents that were notified by institutions to the Office of the Privacy Commissioner for Personal Data, Hong Kong (PCPD) and the number of those that were detected by PCPD through proactive investigations in each of the past six years; the number of incidents involving data processors and the number of persons affected in these two categories of incidents respectively;

(2) as it is learnt that PCPD and the Government are studying amendments to the Personal Data (Privacy) Ordinance, including, among others, establishing a mandatory personal data breach notification mechanism, introducing direct regulation of data processors, empowering the Privacy Commissioner for Personal Data to impose administrative fines, but this Ordinance is not on the list of bills which the Government intends to introduce into this Council in the 2025 session, of the progress made and the legislative timetable for the relevant exercise; and

(3) given that the Government plans to amend the Banking Ordinance with an aim to allow the sharing of information among authorised institutions on customers, accounts and transactions for the purpose of preventing and detecting financial crimes, and the Government indicated in its paper submitted to the Panel on Financial Affairs of this Council in October last year that PCPD had provided its comments on the amendments, of the Government's strategies and measures in place to ensure that the amendments are in line with PCPD's comments while also addressing the surge in the number of fraud cases?

Reply:

President,

In response to the enquiry raised by the Hon Carmen Kan, having consulted the Financial Services and the Treasury Bureau and the Office of the Privacy Commissioner for Personal Data (PCPD), the reply is as follows:

(1) In the past few years, the numbers of personal data breach notifications received by the PCPD and data breach incidents uncovered by proactive compliance checks were relatively stable, amounting to around 100 cases per

year in total. The number witnessed a rising trend up till 2024, to 217 cases. Among those breach incidents, around 10 per cent of them involved malpractice of data processors, and the number of affected persons varied depending on circumstances of individual cases. The relevant statistics may be found at Annex.

(2) In light of the rising trend of personal data breach incidents in recent years, the Government and the PCPD are both deeply concerned about the issue. The PCPD has adopted a multi-pronged approach to tackle the situation, on the one hand updating relevant guidelines and strengthening promotional and educational work, and on the other hand strengthening enforcement work and studying amendments to the Personal Data (Privacy) Ordinance (PDPO) to combat the situation.

With regard to education and publicity work on data security, the PCPD has implemented a series of measures on the following three aspects to raise organisations' awareness in protecting personal data, so as to help organisations reduce the risk of personal data breaches:

(i) Providing "Data Security" tools to support the industries: including (i) launching a one-stop thematic webpage on "Data Security"; (ii) establishing the "Data Security Scanner" for organisations to evaluate their the security level of their data security measures; (iii) introducing a "Data Security Hotline" for receiving enquiries from the industry; (iv) publishing data security guidelines, including "Guidance on Data Breach Handling and Data Breach Notifications" and "Guidance Note on Data Security Measures for Information and Communications Technology", etc;

(ii) Strengthening collaboration with the industry: including (i) organising training talks for organisations to promote data security management, and data security seminars for the public, educational sector and non-profit organisations; (ii) collaborating with the Cyberspace Administration of China, the Hong Kong Police Force, the Digital Policy Office and the Hong Kong Monetary Authority to organise or participate in seminars and activities relating to data security and handling of data breach incidents; and (iii) organising the "Privacy-Friendly Awards" to compliment organisations' outstanding achievements in personal data privacy protection; and

(iii) Organising various promotional activities: including (i) arranging mobile exhibition vehicles to conduct publicity in the community for "Privacy Awareness Week 2024" under the theme of "Safeguard Data Security • Safeguard Privacy"; (ii) introducing "Data Guardian", a data security mascot; (iii) publishing articles in Chinese and English newspapers, online media and professional journals to explain to the public and the industries the importance of data security.

Meanwhile, the PCPD will also strengthen its enforcement efforts – upon confirmation that the relevant data breach incident involves contravention of the PDPO's data security principles, the PCPD will, as appropriate, issue an advisory letter or warning letter to the relevant data user, or serve an enforcement notice on the organisation, directing it to take appropriate remedial measures to prevent recurrence of the situation. If the organisation

does not implement relevant measures in accordance with the enforcement notice, such contravention under the PDPO will constitute an offence, and the maximum penalty is a fine of $50,000 and imprisonment for two years.

With regard to the study of amendments to the PDPO, the PCPD has earlier conducted a comprehensive review of the Ordinance, and its preliminary amendment suggestions include: (1) establishing a mandatory personal data breach notification mechanism; (2) directly regulating data processors; (3) requiring data users to establish a personal data retention period policy; (4) strengthening sanctions and empowering the Privacy Commissioner for Personal Data to hand down administrative fines; (5) clarifying the definition of personal data, etc. On the suggestions above, the PCPD consulted the Personal Data (Privacy) Advisory Committee and the Standing Committee on Technological Developments last year, and listened to the views of different sectors. One of the major concerns of the industry was the strengthened sanctioning powers, and especially their effect and pressure on small, medium and micro enterprises under the current difficult economic situation. The Government fully understands the concerns of the industry. As such, the Government is studying on how to appropriately adjust the legislative amendment proposals, e.g. whether to effect the legislative amendments by phases, thereby reducing the possible effect on business sectors; and how to suitably determine the amount of administrative fines, ensuring they are set at an acceptable level while not losing deterrent effect. The Government is striving to complete the study and come up with concrete legislative amendment proposals at the earliest opportunity, and will consult the Legislative Council, so as to amend the PDPO as soon as possible to further protect the personal data privacy of residents.

(3) To combat fraud and other financial crimes, the Hong Kong Monetary Authority (HKMA) issued a consultation document in January 2024 proposing legislative amendments to the Banking Ordinance to allow sharing of information among banks of information on customer accounts (including personal customers) for the purpose of preventing or detecting crime. The HKMA received 18 separate responses during the consultation period, including comments from the PCPD.

The Government plans to include specific provisions in the legislative amendments which stipulate that banks can share personal accounts information only when there is reasonable suspicion that the personal accounts may be involved in fraud, money laundering or terrorist financing. Banks will be expected to ensure that the relevant requirements are met in each case and be able to demonstrate the grounds on which the decisions are made. In addition, the legislative amendments will also include, amongst others, requirements for banks to keep shared information confidential and to have adequate systems and control measures in place.

Subsequent to the briefing for the Panel on Financial Affairs of the Legislative Council in October 2024, the Government is currently drafting the legislative amendments and will continue to engage the PCPD and other stakeholders to ensure that a balance is struck between fighting against financial crime and safeguarding personal data privacy in the legislative amendments.

Thank you, President.