

LCQ13: Transfer of personal data

\*\*\*\*\*

Following is a question by the Hon Tsang Yok-sing and a written reply by the Secretary for the Civil Service, Miss Denise Yue (in the absence of the Secretary for Home Affairs, Dr Patrick Ho) at the Legislative Council meeting today (March 7):

Question:

It has been reported that some local enterprises intend to outsource information technology jobs to low-cost places, which may involve the transfer of personal data of Hong Kong people to such places. Moreover, section 33 of the Personal Data (Privacy) Ordinance (Cap. 486) regarding "prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances" is not yet in operation. According to the information from the Office of the Privacy Commissioner for Personal Data (PCO), one of the reasons for not putting the provision into operation was to prepare and issue a suitable model contract and relevant guidelines, and it was expected that the relevant provision would come into operation soon after the issuance of the model contract. The PCO had prepared a reference model contract in 1997 and submitted to the Home Affairs Bureau, in June 2005, the investigation report on trans-border dataflow practices in the banking sector in Hong Kong with a range of policy options. In this connection, will the Government inform this Council:

- (a) whether it knows the number of model contracts entered into by data users and data transferees in Hong Kong in the past three years, broken down by the trades of the data transferees;
- (b) of the reasons why the above provision is not yet in operation and the estimated timing of its coming into operation;
- (c) whether the Home Affairs Bureau has discussed with PCO the various options relating to section 33 in the above investigation report;
- (d) of the measures the authorities have in place to prevent the transfer of personal data of Hong Kong people to places outside Hong Kong before the above provision coming into operation, and how they can ensure the protection of personal data of Hong Kong people in places outside Hong Kong (other than encouraging data users

and data transferees to enter into the model contracts); and

(e) whether it has studied the legal provisions concerning the protection of personal data in places (e.g. India and the Mainland) where contractors of outsourced information technology jobs operate?

Reply:

Madam President,

(a) We do not have the statistics on the number of model contracts entered into by data users and data transferees in Hong Kong.

(b) Section 33 of the Personal Data (Privacy) Ordinance (PDPO) prohibits the transfer of personal data from Hong Kong to places that do not have adequate data protection legislation. Commencement of the operation of section 33 would have significant implications on trans-border data transfer activities of various business sectors, notably the banking and telecommunications sectors. We need to have a thorough understanding of the pervasiveness of trans-border data flows, as well as the processes involved in the transfer of personal data and the issues pertaining to its protection that organizations may encounter when engaging in offshore outsourcing. The Privacy Commissioner for Personal Data (the Commissioner) is undertaking a comprehensive review of the entire Ordinance, including section 33. We shall examine the Commissioner's recommendations and then map out the best way forward taking into account the interests of relevant stakeholders.

(c) The Home Affairs Bureau has been in discussion with the Commissioner on the policy options put forward in the investigation report on trans-border dataflow practices in the banking sector in Hong Kong. We pointed out to the Commissioner, amongst other things, that the commencement of the operation of section 33 would hinge on two key factors, namely his readiness to specify in a gazette notice places with legislation substantially similar to, or serving the same purposes as the PDPO, as stipulated in sub-section 33(3), and his readiness to repeal or amend such notice as stipulated in sub-section 33(4). The practicality of the existing section 33 will also be looked into in the comprehensive study currently conducted by the Commissioner. Separately, the Commissioner has joined the APEC Cross-Border Rules Study Group which is tasked to develop cross-border privacy rules to facilitate responsible and accountable cross-border information flows without creating unnecessary barriers.

Participation in the Study Group could provide insights for Hong Kong in tackling the issues relating to regulation of trans-border data flow under section 33 of the PDPO.

(d) Use of personal data, including transfer, is regulated by Data Protection Principle 3 of the PDPO. Unless the transfer of personal data is for a purpose same as or directly related to the original purpose of collection of such data, a data user is not allowed to transfer such personal data to a place outside Hong Kong without the consent of the data subject. A data user who has transferred personal data to a place outside Hong Kong must comply with the requirements of the PDPO if the data user can control the holding, processing or use of the data. According to section 65 of the PDPO, any act done or practice engaged in by a person as agent for another person with the authority (whether express or implied, and whether precedent or subsequent) of that other person shall be deemed under the PDPO as done or engaged in by that other person as well as by him. As such, the data user shall be accountable for any contravention of the Ordinance committed by its offshore agent (e.g. a bank which commissions an offshore agent to process the personal data of its customers on its behalf is accountable for any contravention of the PDPO committed by the agent). A data user who has contravened a data protection principle of the PDPO may be served an enforcement notice by the Commissioner. Contravention of an enforcement notice is an offence and is liable on conviction to a fine at level five (up to \$50,000) and to imprisonment for two years, and in the case of a continuing offence, to a daily penalty of \$1,000. A data user who contravenes any requirement (other than a data protection principle) under the PDPO is liable on conviction to a fine at level three (up to \$10,000), and depending on the nature of offence, an imprisonment for six months also.

(e) To our knowledge, there is no law regulating the protection of personal data privacy in the Mainland and India.