LCQ6: Protection of personal data privacy

Following is a question by the Hon Elizabeth Quat and a reply by the Secretary for Innovation, Technology and Industry, Professor Sun Dong, in the Legislative Council today (May 29):

Question:

There are views that the incidents of personal data breaches or hacker intrusions that have occurred in recent years in a number of government departments and public and private organisations reflect a generally low awareness among society about protecting personal data and ensuring cyber security. In this connection, will the Government inform this Council:

(1) whether it will instruct the heads of various government departments and the heads of information technology security of such departments be held accountable for the security work of the computer systems in their departments, and take disciplinary actions against officers involved in cases of human negligence or non-compliance;

(2) given that the Office of the Privacy Commissioner for Personal Data, Hong Kong indicated in its paper submitted to the Panel on Constitutional Affairs of this Council in February this year that it was working with the Government to conduct a comprehensive review of the Personal Data (Privacy) Ordinance and formulate concrete legislative amendment proposals, including the establishment of a mandatory notification mechanism for breach of personal data, of the latest progress of the relevant work and the specific timetable; whether the Government will introduce mechanisms such as administrative fines under the Ordinance, and step up the relevant education and promotion efforts to raise the awareness of cyber and information security in society as a whole; and

(3) whether it will study the introduction of data privacy assessments and audits for all government information technology projects, so as to ensure that the relevant systems will not disclose excessive and unnecessary personal data to the public?

Reply:

President,

Information and cyber security are the cornerstone of digital government. All bureaux and departments (B/Ds) are responsible for ensuring the primary security of their information technology (IT) systems and data, and should put in place effective information security framework and specific measures for their systems in accordance with the Government Information Technology Security Policy and Guidelines issued by the Office of the Government Chief Information Officer (OGCIO).

The recent incidents of personal data breach of individual government departments and public organisations show that B/Ds as well as all sectors of society must stay vigilant about information and cyber security risks at all times, and should continuously strengthen the protection of information systems and data.

Regarding the three parts of the question, in consultation with the Constitutional and Mainland Affairs Bureau (CMAB), my reply is as follows:

(1) Under the existing Policy and Guidelines, B/Ds are directly responsible for the implementation and security of their IT projects. The scope of their main responsibilities include the following:

(i) Comply with and adopt the information security risk management system, technical requirements and reference standards as stated in the Policy and Guidelines;

(ii) Supervise the implementation of their IT systems and ensure that relevant personnel adhere to the Policy and Guidelines;

(iii) Conduct regular security risk assessments and audits (SRAA) for their IT infrastructure, information systems and data assets;

(iv) Report information security incidents to the Government Information Security Incident Response Office, and notify as appropriate the Office of the Privacy Commissioner for Personal Data (PCPD) and/or the Police depending on the nature of incident; and

(v) Government officers should strictly follow the other applicable rules and regulations, including the Security Regulations, the Official Secrets Ordinance and the Civil Service Code.

It is clear that B/Ds shoulder the responsibility of the first line of defence to safeguard the security of IT systems under their purview. The heads of B/Ds will handle cases in accordance with the established procedures if their personnel or contracted service providers are suspected of violating relevant regulations or engaging in illegal acts.

To further enhance the key supervisory role of B/Ds over government IT projects, the OGCIO is actively examining measures to provide appropriate guidance and technical support to B/Ds, such as requiring B/Ds to designate senior officers to directly supervise the SRAA of their information systems, and to strengthen the cyber risk detection, spot checks and compliance audits. We will implement relevant measures as soon as possible.

(2) According to information provided by the CMAB, the PCPD is currently conducting a comprehensive review of the Personal Data (Privacy) Ordinance (Ordinance) and formulating concrete proposals for legislative amendments, which include establishing a mandatory personal data breach notification mechanism, requiring data users to formulate policies on personal data retention period, empowering the Privacy Commissioner for Personal Data to

impose administrative fines, direct regulation of data processors, and clarifying the definition of personal data. The PCPD is studying in detail relevant laws of other jurisdictions while taking account of the actual situation in Hong Kong, so as to put forward practicable legislative amendment proposals to align with international developments in privacy protection and strengthen the protection of personal data privacy. Once specific legislative amendment proposals are firmed up, the PCPD will consult the Government and the Legislative Council, after which a legislative amendment timetable will be drawn up having regard to actual circumstances.

In addition, the PCPD has been actively engaging in publicity and education work in different aspects, with a view to promoting and enhancing public awareness of personal data security. These efforts include launching a thematic webpage on data security and a data security hotline to help enterprises enhance their measures on safeguarding data security; organising and participation in various seminars and conferences to elaborate on cyber security and data security measures; and rolling out the flagship promotional event Privacy Awareness Week 2024 under the theme of "Safeguard Data Security • Safeguard Privacy", with a view to improving the capability of the public and organisations in safeguarding personal data.

The Policy and Guidelines requires all B/Ds to conduct privacy impact assessment (PIA) during the design stage of information systems and before making updates of significant impact, which help identify and address early the potential privacy issues in the information systems. In response to the latest developments in information and cybersecurity, the OGCIO is studying measures to require B/Ds to appoint senior officers to closely oversee the PIA of their information systems. It will also introduce regular testing, cyber security attack and defence drills, enhanced staff training and closer collaboration with stakeholders, so as to strengthen the abilities to monitor and safeguard for government information systems, thereby protecting more effectively the information systems and data security.