LCQ9: Data governance system

Following is a question by the Hon Carmen Kan and a written reply by the Secretary for Innovation, Technology and Industry, Professor Sun Dong, in the Legislative Council today (November 15):

Question:

Regarding the data governance system, will the Government inform this Council:

(1) given that as proposed in the latest Policy Address, the Government will publish administrative guidelines to facilitate data flow and ensure data security before the end of 2023, of the nature of the administrative guidelines; as there are views that data flow and data security are only two of the essential elements of the data governance system, whether the authorities will consider enacting comprehensive regulations on data governance; if so, of the details; if not, the reasons for that;

(2) given that as stated in the latest Policy Address, the Government (i) signed a Memorandum of Understanding with the Mainland authorities in June 2023 to foster secure crossâ€‘boundary flow of Mainland data within the Guangdong-Hong Kong-Macao Greater Bay Area (GBA) and (ii) is liaising with the authorities of the Guangdong Province to adopt an early and pilot implementation approach in the GBA to streamline the compliance arrangements for the flow of personal data from the Mainland to Hong Kong in order to facilitate the provision of crossâ€‘boundary financial and medical services within the GBA, whether the authorities have plans to drive the flow of people, goods and capital within the GBA by the flow of information; if so, of the specific plans and timetable for the relevant measures; if not, the reasons for that;

(3) as the Government indicated in reply to a question raised by a Member of this Council on June 7, 2023 that it might not be necessary to centralise all the data on one platform, and the Government would develop the Consented Data Exchange Gateway (CDEG) to facilitate the interflow of data among government departments, with the target of rolling out CDEG by the end of 2024, of the latest progress of the relevant work; and

(4) in tandem with facilitating data interchange to foster the development of the innovation and technology industry, the financial industry, etc. (for example, the Commercial Data Interchange of the Hong Kong Monetary Authority will be connected to CDEG by the end of 2023), of the safeguards for cyber and data security the authorities have in place to realise the vision of secure flow and orderly sharing of data?

Reply:

President,

Having consulted the Security Bureau, Financial Services and the

Treasury Bureau and the Hong Kong Monetary Authority (HKMA), my reply to the questions raised by the Hon Carmen Kan is as follows:

(1) Data governance encompasses multiple elements, including the integration, application, opening up and sharing of data; data security; infrastructure; industry development; and alignment with different standards and regulatory frameworks. The Government has been developing a data governance system that suits the circumstances of Hong Kong under a multi-pronged strategy covering policies, legislation, guidelines, infrastructure, etc.

Data flow and data security are key elements in promoting and enhancing data governance. In this regard, "The Chief Executive's 2023 Policy Address" announced that the Government will publish administrative guidelines to facilitate data flow and ensure data security, with the objective to elaborate on our management principles and strategies concerning the relevant elements of data governance and to propose an action plan for further promoting the interchange of data and related security safeguards, covering areas like top-level design, policies, guidelines, regulations, infrastructure, and cross-boundary data flow. We will publish the aforementioned management measures by the end of this year.

(2) Facilitating the secure cross-boundary flow of Mainland data in the Guangdong-Hong Kong-Macau Greater Bay Area (GBA) is a key initiative to promote the development of digital economy and smart city in the three places. The Innovation, Technology and Industry Bureau and the Cyberspace Administration of China entered into the Memorandum of Understanding on Facilitating Cross-boundary Data Flow Within the Guangdong-Hong Kong-Macao Greater Bay Area (MoU) in June 2023, with a view to fostering the safe and orderly flow of Mainland data to Hong Kong under the national management framework on safeguarding the security of cross-boundary data. This initiative will not only reduce the compliance costs of cross-boundary data flow for enterprises, but will also promote the digital economy and scientific research development in the GBA, and thus is conducive to facilitating Hong Kong's integration into the GBA and the nation's overall development, as well as building Hong Kong into an international data hub.

In accordance with the framework set out in the MoU, the Office of the Government Chief Information Officer (OGCIO) is liaising with the Cyberspace Administration of Guangdong Province to strive for adoption of the early and pilot implementation approach as soon as possible to streamline the compliance arrangements for personal information flow from the Mainland to Hong Kong. The initial early and pilot implementation arrangement is expected to be first applied to high-demand cross-boundary services such as finance, credit checking and healthcare, so as to promote the provision of relevant cross-boundary services in the GBA and bring convenience and facilitation to the public and businesses. We will consider extending the facilitation measure to other sectors in an orderly manner having regard to the effectiveness and experience in the first stage of the pilot implementation of the arrangements.

(3) OGCIO is developing the Consented Data Exchange Gateway (CDEG) and will introduce in the first instance the function of interfacing with the HKMA's

Commercial Data Interchange (CDI) by end-2023 to facilitate the sharing of data from government departments to financial institutions upon the authorisation of their enterprise clients. OGCIO will roll out other functions of CDEG before end-2024 for citizens to authorise government departments to share their personal data within the government to facilitate their use of digital government services. Following enhancement to the functionalities of "iAM Smart" platform and by providing one-time authorisation on "iAM Smart", citizens can in future make use of CDEG to directly access their personal information in various government services and leverage the "iAM Smart" e-ME function for auto-filling of personal information when applying for other government services, hence obviating the need for repetitive input or submission of the same information, thereby realising the goal of achieving a "single portal for online government services".

(4) The Government has devised a multi-layered mechanism on data security protection while promoting the sharing and application of data. The mechanism focuses on data governance, classification, grading, protection, audit, risk assessment, monitoring and contingency plans, etc.

For instance, CDEG will not store any data shared between bureaux and departments (B/Ds). The shared data will only be saved on respective systems of B/Ds, which are required to conduct regularly risk assessment and audit concerning their information systems and data security to safeguard the government systems and data security. With regard to online transmission, CDEG will be linked to the systems of various B/Ds and the CDI with encryption. CDEG will also utilise the Shared Blockchain Platform of OGCIO to ensure that the records of authorisation by citizens and data sharing between B/Ds cannot be tampered. When developing the CDEG, OGCIO had consulted the Office of the Privacy Commissioner for Personal Data and engaged independent third parties to conduct security risk assessments and audit as well as privacy impact assessments to ensure compliance with the Personal Data (Privacy) Ordinance.

On the other hand, for CDI launched by the HKMA, there are rules requiring participating banks to ensure that the scope and use of data collected comply with the purposes agreed by the small and medium enterprises (SMEs) as owners of the data. At the technical level, CDI connects banks and data providers with encryption, while the commercial data will not be stored in the system of CDI. A number of corresponding information security requirements are also put in place to protect the privacy of SMEs and to ensure data security. Meanwhile, CDI has a strict regulatory mechanism to protect customers.

To address potential security risks associated with critical infrastructure in different sectors, the Critical Infrastructure Security Coordination Centre (CISCC) and the Cyber Security Centre (CSC) of the Police Force operate round the clock. The CISCC seeks to strengthen self-protection and restoration capabilities of the critical infrastructure through public-private sector co-operation, risk management, on-site security inspections, etc. Meanwhile, the CSC conducts timely cyber threat audits and analyses to prevent and detect cyber attacks against the critical infrastructure.

At the same time, the Government will strive to enhance the protection of cybersecurity of critical infrastructure (including energy, telecommunications, transportation, financial institutions). Among other things, the Government will enact legislation to stipulate the cybersecurity obligations of critical infrastructure operators. The Government is working on the legislative proposals and will consult the Panel on Security of the Legislative Council (LegCo) and relevant stakeholders in due course. The target is to introduce the bill into the LegCo within 2024.