

## **Forty-ninth Meeting of the Business Facilitation Advisory Committee**

### ***Agenda Item 3 : The Role of the Office of the Privacy Commissioner for Personal Data in Assisting Businesses and Organisations to Enhance Data Governance***

#### **Purpose**

This paper provides Members of the Business Facilitation Advisory Committee (BFAC) with an overview of the functions and structure of the Office of the Privacy Commissioner for Personal Data (PCPD), and introduces its role in assisting businesses and organisations to enhance data governance.

#### **Background**

2. The PCPD is an independent body set up to oversee the implementation of and compliance with the provisions of the Personal Data (Privacy) Ordinance (Chapter 486 of the Laws of Hong Kong) (PDPO). The PCPD strives to ensure the protection of the privacy of individuals in relation to personal data through monitoring and supervising compliance with the PDPO, enforcing its provisions and promoting the culture of protecting and respecting personal data.

3. Established in August 1996, the PCPD is headed by the Privacy Commissioner for Personal Data (Privacy Commissioner). It comprises different functional units, including the Complaints Division, Criminal Investigation Division, Compliance & Enquiries Division, Legal Division, Global Affairs & Research Division, Corporate Communications Division and Corporate Support Division.

#### **Data Breach Incidents and the Role of the PCPD**

4. Data Protection Principle (DPP) 4(1) of Schedule 1 to the PDPO requires a data user to take all practicable steps to ensure that any personal data held by the data user is protected against unauthorised or accidental access, processing, erasure, loss or use. In general, a data breach occurs

when there are inadequate security or vulnerabilities of the personal data held by a data user, thereby exposing the data to the risks of unauthorised or accidental access, processing, erasure, loss or use, and the breach may be found to be in contravention of DPP 4. From January to September 2022, the PCPD received 85 personal data breach notifications. In 2021, the PCPD received a total of 140 notifications, which represented an increase of 36% when compared to 103 in 2020.

5. All along, the PCPD calls on organisations to notify the PCPD of any data breach incident as soon as possible. Notification of a data breach incident will enable the PCPD to help the organisation and the affected parties to take appropriate and timely measures to minimise the damage caused by the incident to the organisation and the affected parties. The organisation should also notify the affected parties of the data breach incident as soon as possible.

6. Pursuant to section 8(1) of the PDPO, the Privacy Commissioner shall monitor and supervise compliance with the provisions of the PDPO, and promote awareness and understanding of, and compliance with, the provisions of the PDPO. In case the PCPD finds that an organisation's practices do not comply with the requirements of the PDPO, the PCPD would decide whether the situation warrants a compliance check or an investigation into the matter. When the compliance check is completed, the Privacy Commissioner would generally advise on the deficiencies identified and make suggestions for remedial actions to prevent and avoid recurrence of similar incident. From January to September 2022, the PCPD initiated 311 compliance checks. In 2021, the PCPD initiated a total of 377 compliance checks, representing an increase of 10% when compared to 344 in 2020.

7. In addition, section 36 of the PDPO also empowers the Privacy Commissioner to carry out an inspection of personal data system used by a data user, either by itself or a class of data users. In the light that public utility companies handle a vast amount of customers' data in their normal business of maintaining service accounts, processing bills and handling customer enquiries, the Privacy Commissioner carried out inspections of the customers' personal data systems of CLP Power Hong Kong Limited and The Hongkong Electric Company, Limited in 2021 and published an inspection report in August of the same year.

8. Given that data users are confronted with considerable challenges to the protection of personal data privacy, the PCPD issued the "Guidance

Note on Data Security Measures for Information and Communications Technology” in August 2022 to provide data users with recommended data security measures for information and communications technology (ICT) to facilitate their compliance with the requirements of the PDPO.

### **Addressing Privacy Issues Raised in relation to COVID-19**

9. For over two years, different parts of the world have been hard hit by the COVID-19 pandemic. Governments worldwide have been introducing different policies and solutions to combat the pandemic and address the challenges posed by it, such as contact tracing, imposition of regulations on cross-border travels, implementation of vaccination campaigns and Vaccine Pass, and the like. The PCPD has been keeping abreast of the developments both internationally and in Hong Kong in this regard. We provided advice and guidance from the perspective of the protection of personal data privacy to relevant stakeholders in the introduction of new initiatives to combat the pandemic and on our road to recovery. By the end of September 2022, the PCPD has issued 23 guidelines/media statements on the COVID-19 pandemic, including the “Guidance for Employers on Collection and Use of Personal Data of Employees during COVID-19 Pandemic”, the “Protecting Personal Data under Work-from-Home Arrangements” guidance and leaflet, etc.

### **Artificial Intelligence and Development of the Guangdong-Hong Kong-Macao Greater Bay Area**

10. Hong Kong is dedicated to becoming a technology and data hub in the Guangdong-Hong Kong-Macao Greater Bay Area and the Asia Pacific region. In line with the Outline Development Plan for the Guangdong-Hong Kong-Macao Greater Bay Area, the healthy development and use of artificial intelligence (AI) can help Hong Kong leverage its strengths as a regional data hub, as well as empower Hong Kong to become a technology and innovation centre and a world-class smart city. While AI has huge potentials in boosting productivity and economic growth, the use of AI also brings with it challenges to the protection of personal data privacy. Against this backdrop, the PCPD issued the “Guidance on the Ethical Development and Use of Artificial Intelligence” in August 2021 to help organisations understand and comply with the relevant requirements of the PDPO when they develop or use AI.

## **Privacy Regulations in the Mainland**

11. Regulatory overhauls are not confined locally. The Personal Information Protection Law (PIPL), the first piece of legislation on the Mainland dedicated to protecting personal information, came into effect in November 2021. To help the general public and businesses in Hong Kong better understand the regulatory regime for the protection of personal information on the Mainland, the PCPD published a booklet entitled “Introduction to the Personal Information Protection Law of the Mainland” shortly after the PIPL came into effect. As part of our educational efforts, the PCPD also organised webinars to introduce the latest regulatory developments in the Mainland in this regard, including “The Mainland’s Security Assessment Measures on Cross-border Transfers of Data” which came into operation in September 2022.

## **Industry-specific Privacy Campaigns**

12. The PCPD has been collaborating with different industries to promote the awareness of the protection of personal data privacy. In 2022, the PCPD organised two webinars on “Protection of Personal Data Privacy for Property Management Sector”; gave a presentation on “Data Security Management in the Cyber World – Practical Tips on Personal Data Security and Incident Response” for the ICT sector; and organised thematic webinars for sectors like banking, insurance and legal. The PCPD also provided tailor-made training sessions to different organisations and help them meet their compliance and operational needs.

## **Personal Data Privacy Management Programme**

13. The PCPD issued the “Privacy Management Programme: A Best Practice Guide” with a view to assisting organisations in establishing a comprehensive privacy management system. The Privacy Commissioner advocates that organisations should develop their own Personal Data Privacy Management Programme (PMP) and appoint a Data Protection Officer in order to institutionalise a system for the responsible use of personal data that is in compliance with the PDPO. Organisations are advised to embrace personal data protection as part of their corporate governance responsibilities and apply them as a business imperative throughout the organisation, starting from the boardroom.

14. The appointment of Data Protection Officers is an important component of a PMP. Established by the PCPD in 2000, the Data Protection Officers' Club (DPOC) has been dedicated to providing data protection practitioners from the public and private sectors with an effective training and experience-sharing platform, which allows members to acquaint themselves with information about the latest developments in the privacy landscape and personal data privacy protection, and also enhance their compliance with relevant regulations. The DPOC membership reached more than 500 by the end of September 2022, with members coming from diverse backgrounds, including human resource management and training, compliance, legal, regulatory and law enforcement.

### **Advice Sought**

15. Members of the BFAC are invited to note the content of the paper.

**Office of the Privacy Commissioner for Personal Data  
November 2022**