I. APPLICABLE LAWS AND REGULATIONS

Hong Kong has enacted a detailed law and a series of administrative codes governing data privacy issues. The primary privacy law in Hong Kong is the Personal Data (Privacy) Ordinance (Cap. 486) (PDPO). The only section of the PDPO which has not yet been brought into force is Section 33, which concerns the cross-border transfer of personal data (see IV.D, below). The administrative body charged with overseeing the enforcement of the PDPO is the Office of the Privacy Commissioner for Personal Data (PCPD).

The PDPO regulates any data relating directly or indirectly to a living individual, from which it is practicable for the identity of that individual to be directly or indirectly ascertained, in a form in which access to or processing of the data is practicable (“personal data” as defined in § 2(1)). Any person who controls the collection, holding, processing, or use of personal data in Hong Kong (“data user” as defined in § 2(1)) is subject to the provisions of the PDPO. The PDPO imposes requirements and restrictions on data users concerning the collection, use, processing, transfer, and storage of personal data (Schedule 1, Data Principles 1–6), and grants to individuals who are the subject of the personal data (“data subject” as defined in § 2(1)) the right to access and correct their personal data held by a data user (Part 5). The PDPO provides some limited exemptions to the restrictions imposed by it (see, e.g., §§ 20–21 and 24–25, related specifically to data access and correction, and Part 8, which contains a number of exemptions).

Recently, amendments were made to the PDPO by the Personal Data (Privacy) (Amendment) Ordinance (Amendment Ordinance), which was enacted in June 2012 and came into effect in October 2012 and April 2013. Some of the major changes introduced by the Amendment Ordinance addressed the use of personal data in direct marketing activities (Part 6A), which came into effect on April 1, 2013. These provisions outline stringent requirements that data users must comply with in order to use personal data to conduct direct marketing activities aimed at data subjects, or to provide personal data to third parties for their own direct marketing purposes.

Some of the criminal law ordinances augment the PDPO on the issue of cybersecurity. Specifically, the Computer Crimes Ordinance, enacted in 1993, amended specific provisions of the Telecommunications Ordinance (Cap. 106, § 27A), the Crimes Ordinance (Cap. 200, §§ 59, 60, 85, and 161), and the Theft Ordinance (Cap. 210, §§ 11 and 19) to create new computer-related offenses. For example, it is an offense to gain unauthorized access to a computer with the intent to commit an offense or with an otherwise dishonest intent, to misuse a computer belonging to another, or to enter into a building as a trespasser to unlawfully alter or erase any program or data held in a computer.

The PCPD has issued a number of Codes of Practice, Guidance Notes, and Information Leaflets to assist data users in complying with their obligations under the PDPO. These include the Code of Practice on Human Resource Management (HR Code) and the Code of Practice on the Identity Card Number and other Personal Identifiers (ID Code). These guidance documents do not carry the force of law. However, the failure to abide by them will likely be taken into account by the PCPD in assessing whether a data user has complied with the PDPO. In particular, pursuant
to PDPO § 13(2), any noncompliance with a Code of Practice will give rise to a presumption against the data user in an action brought before the Privacy Commissioner, and any court or administrative appeal board may take the failure into account in determining whether a data user has violated the PDPO.

II. REGULATORY AUTHORITIES AND ENFORCEMENT

Among its many responsibilities, the PCPD investigates potential breaches of the PDPO by data users, either based on its own initiative or in response to complaints, to ensure that issues are resolved fairly and that data users meet their data protection obligations. In addition, the PCPD educates individuals and data users on best practices and promotes such practices through publications and media outlets. Along with the HR Code and the ID Code noted above, the PCPD has issued Privacy Guidelines: Monitoring and Personal Data Privacy at Work (Employee Monitoring Guidelines), Code of Practice on Consumer Credit Data, Guidance on Use of Data Obtained From the Public Domain, and Understanding the Code of Practice on Human Resources Management: Frequently Asked Questions About Recruitment Advertisements. In January 2013, the PCPD issued guidelines on the latest changes to the PDPO concerning direct marketing activities (New Guidance on Direct Marketing). The direct marketing restrictions imposed by the PDPO relate to the sending of marketing materials addressed to specific named individuals (e.g., John Smith), by any means of communication (e.g., by post, e-mail, fax, etc.). However, marketing materials that are not specifically addressed to named individuals (e.g., addressed to “the occupant” rather than “John Smith”) are not regulated by the PDPO—such marketing activities if sent by electronic means, such as e-mail (usually referred to as “spam”), are instead regulated under the provisions of the Unsolicited Electronic Messages Ordinance (Cap. 593) (UEMO).

In the event that the PCPD receives a complaint from an individual or discovers that a PDPO violation may have occurred, it has the power to conduct an investigation. The authority of the PCPD is quite broad, as set forth in PDPO Part 7. Among other powers, the PCPD may inspect a data user’s personal data system and may enter the premises of a data user to complete any inspection or investigation. If following the completion of an investigation the PCPD finds that a data user has contravened the provisions of the PDPO, the PCPD may issue an enforcement notice specifying the remedial steps that must be taken by the data user to rectify the violation and to prevent any recurrence. Data users who contravene such a notice commit an offense and are liable for a level 5 fine (HK$50,000) and two years' imprisonment on first conviction, plus a daily fine of HK$1,000 if the offense continues. On a second or subsequent conviction, the penalty is increased to a level 6 fine (HK$100,000) and two years' imprisonment, with a daily fine of HK$2,000 if the offense continues. A data user who, after having complied with an enforcement notice, contravenes the PDPO by committing the same acts or omissions is liable on conviction for a level 5 fine (HK$50,000) and two years' imprisonment, with a daily fine of HK$1,000 if the offense continues (without the PCPD needing to issue a further enforcement notice) (PDPO § 50A).

The sanctions for a violation of the PDPO’s restrictions on the use of personal data for direct marketing purposes are even more severe. For example, data users using a data subject's personal data for their own direct marketing purposes in contravention of the PDPO requirements are, in most cases, subject to a fine of HK$500,000 and three years' imprisonment (PDPO §§ 35C–35G). However, any data user that, in return for gain, provides personal data to a third party for use by that third party for its own direct marketing purposes, in contravention of the PDPO, is subject to a fine of HK$1,000,000 and 5 years' imprisonment. The penalty is reduced to HK$500,000 and three years if the personal data is provided to the third party other than for gain (PDPO §§ 35J–35L).

III. RISK ENVIRONMENT

Following a number of highly publicized data privacy breaches in Hong Kong in the year 2010, the public's awareness of data privacy rights significantly increased, and the PCPD became proactive in taking action against data users for infringement of the PDPO and also in issuing Guidance Notes and Information Leaflets to assist in compliance with the PDPO.

The number of complaints received by the PCPD has been steadily increasing. From April 2001 to
March 2002, the PCPD received 888 complaints. In 2015, it received a record high of 1,971 complaints, up 16% from the previous year. The number of enforcement notices issued by the PCPD has been less stable. In 2015, the PCPD issued 67 enforcement notices, as compared with 90 in 2014 and 25 in 2013. The PCPD initiated 76 investigations in 2015, down from the 102 it initiated in 2014, but still well above the 19 from 2013. The PCPD is clearly taking a proactive approach to ensure compliance with data protection obligations.

Additionally, 2014 marked the first time a prison sentence was issued by the Hong Kong courts for a breach of the PDPO. In that case, an insurance agent was sentenced to four weeks' imprisonment for knowingly making a false statement to the PCPD. In 2015, there were six prosecutions by the court for breaches of the PDPO, and 30 cases were referred by the PCPD to the police for criminal investigation and prosecution. Four of the convictions in 2015 related to breaches of the direct marketing provisions under the PDPO. The PCPD is likely to continue to refer cases to the Hong Kong courts for prosecution, and given the continuing increase in public concern regarding data privacy, it is likely that the Hong Kong courts will also take a firmer approach against offenders. See “First Prison Sentence Imposed Under Personal Data (Privacy) Ordinance,” World Data Protection Report (Jan. 23, 2015).

The PCPD does not take a back-seat approach to compliance with the PDPO, and any noncompliance by a data user will run the risk of coming under the scrutiny of the PCPD. Even though in some circumstances breach of the PDPO will not result in an automatic offense, and data users will be given the chance to rectify a breach in compliance with an enforcement notice, the biggest risk to a data user is damage to its reputation. The PCPD has the power to (and often does) “name and shame” data users who have breached the PDPO. This could have serious consequences for a data user's business, particularly if the business relies heavily on the customer's trust or it collects and uses particularly sensitive personal data (e.g., health records, bank account details, or HKID card numbers).

**IV. EMERGING ISSUES AND OUTLOOK**

### A. Current Enforcement Emphases

The PCPD announced that for 2016, it will specifically focus on:

- (a) monitoring global data protection developments and conducting comparative research and analysis on topics such as big data and the Internet of things;
- (b) promoting the Privacy Management Programme;
- (c) educating the public about the PDPO and the activities of the PCPD;
- (d) supporting the operation of the Electronic Health Record Sharing System; and
- (e) reviewing international developments and assessing whether changes to the PDPO are needed in light of these developments.

See PCPD Media Statement (Jan. 26, 2016).

The PCPD's focus usually corresponds with topically issues, particularly regarding the emergence of new technology. For example, it decided in 2016 to carry out research on the Internet of things in response to the challenges it raises in the digital age. Previously, the PCPD had been focused on other digital and information technology related issues, including the use of mobile applications. In November 2012, the PCPD issued an Information Leaflet on Personal Data Privacy Protection: What Mobile App Developers and their Clients Should Know. In November 2014, the PCPD then issued a Best Practice Guide for Mobile App Development. The PCPD has also carried out investigations into mobile apps, the most highly reported of which concerned an investigation into the mobile app “Do No Evil” (PCPD Media Statement (Aug. 13, 2013)). Keeping abreast with technology, the PCPD also issued in March 2015 an updated Guidance Note on CCTV Surveillance and the Use of Drones.

The collection and use of personal data that is publicly available on public registers has also received attention from the PCPD since 2013. In the “Do No Evil” investigation, the Privacy Commissioner published an investigation report regarding the mobile app, which involved the collection and compiling of individuals' litigation and bankruptcy information from public registers to enable users to search for such data with respect to specific individuals. The PCPD found that the app was in serious breach of the PDPO, and an enforcement notice was issued against the developer. The PCPD also issued Guidance on Use of Personal Data Obtained from the Public Domain in August 2013. More recently, in October 2015, the Hong Kong Administrative Appeals Board dismissed an appeal made by Mr. David Webb against an enforcement notice issued by the PCPD requiring him to remove from his website certain hyperlinks to publicly available anonymised judgments. See “Navigating the Hong Kong Web—A Private or Public Affair?,” Privacy Law Watch (April 18, 2016). The PCPD will most likely continue to take active
steps in this area by conducting self-initiated investigations and compliance checks, as well as hosting further seminars and workshops to help educate organizations.

**B. Electronic Health Record Sharing System Ordinance**

On Dec. 2, 2015, the **Electronic Health Record Sharing System Ordinance** (EHRSSO) came into effect. The EHRSSO allows health-care professionals and public and private hospitals to collect, share, and store patients' electronic health records via the **Electronic Health Record Sharing System** (eHRSS), which was launched on March 7, 2016. Participation in the eHRSS is voluntary, but all of Hong Kong's local private hospitals have registered to join eHRSS, and as of March 10, 2016, more than 240 healthcare providers of the pre-existing Public-Private Interface – Electronic Patient Record Sharing Pilot Project (PPI-ePR) have applied to join eHRSS. See “**Electronic Health Record Sharing System commences operation,**” Press Release (March 13, 2016). See also “**Sharing is Caring: New Electronic Health Record Sharing System for Hong Kong,**” World Data Protection Report (April 28, 2016).

**C. Privacy Compliance Framework**

The Privacy Management Programme (PMP) was promulgated by the PCPD in February 2014 to establish a strategic framework that can be used by data users to install a robust privacy infrastructure supported by an ongoing review and monitoring process to ensure compliance with the PDPO (See **PMP Best Practice Guide**). One of the primary goals of the PMP is to urge data users to embrace personal data policies as an integral component of their corporate governance responsibilities. The PCPD will continue to encourage and assist organizations' adoption of the PMP.

**D. International Data Transfers**

The PCPD has not expressly identified PDPO Section 33 as an area of focus for 2016. When the PDPO was enacted, Section 33 was designed to deal with international data transfers. This provision prohibits the transfer of personal data from Hong Kong to another jurisdiction unless one of the limited, specified exceptions applies. For example, a data user would be able to transfer personal data to a country outside of Hong Kong if the data subject had consented to such cross-border transfer or the transfer was to a jurisdiction included in a “white list” to be formulated by the PCPD (i.e., a list of jurisdictions that the PCPD considered to have data privacy laws substantially similar to, or serving the same purpose as, the PDPO). Section 33 is still expected to come into operation, although there is no indication of when that will happen. In December 2014, the PCPD issued its **Guidance on Personal Data Protection in Cross-Border Data Transfer**, which is designed to give data users information on their compliance obligations and to prepare them for Section 33 eventually coming into force. However, recent discourse from the new Privacy Commissioner (who took office in August 2015) appears to indicate that Section 33 will not be brought into operation anytime in the near future.