Data. Protection. Adding Value.

Data Protection Laws - Hong Kong

Legislation

The Personal Data (Privacy) Ordinance (Cap. 486) ("**PDPO**") was enacted on 3 August 1995 and took effect on 20 December 1996. The objective of the PDPO is to protect the privacy rights of individuals with regard to their personal data. It regulates the collection, processing, and use of personal data by both the public and private sectors.

Scope: The PDPO applies to "data users" who controls the collection, holding, processing or use of the data in or from Hong Kong. Although the PDPO does not contain any express provisions conferring extra-territorial application, overseas organizations operating in Hong Kong must still comply with the PDPO.

Key Exemptions:

- Crime prevention or prosecution, security and defence, statistics and research, news activity, protecting a data subject's health etc.
- The use of personal data is required or authorised by law or court order or is required for exercising or defending legal rights in Hong Kong
- Domestic purposes

Risk Level: Medium

Supervisory Authority & Registration

Supervisory Authority: The Office of the Privacy Commissioner for Personal Data ("**PCPD**") is the supervisory authority and an independent statutory body which oversees the enforcement of the PDPO in Hong Kong. The PCPD aims to secure the protection of privacy of the individual with respect to personal data through promotion, monitoring and supervision of compliance with the PDPO.

Registration/Approval Requirements: Currently, organizations that collect and handle personal data in Hong Kong are not subject to any particular registration requirements. Nonetheless, the PDPO grants the power to PCPD to impose registration and reporting obligations on certain categories of organizations (although there are not such requirements to date).

Data Protection Principles ("DPP")

Any person or organization collecting, handling or using personal data must comply with the following DPPs:

DPP 1 – Purpose and Manner of Collection

- Personal data must be collected for a lawful purpose on a necessary basis and the means of collection should also be lawful and fair.

DPP 2 – Accuracy and Duration of Retention

- Data users must ensure that the data held are accurate and not kept longer than is necessary for the consented purpose.

DPP 3 – Use of Data

- Data must not be used for any purpose other than the one mentioned at the time the data were collected (or a directly related purpose), unless with consent.

DPP 4 – Data Security

- Data users must take appropriate security measures to protect personal data.

DPP 5 – Openness and Transparency

- Data users must publicly disclose the kind (not the content) of personal data held by them and their policies and practices on how they handle personal data.

DPP 6 – Access and Correction

- A data subject is entitled to ask a data user whether or not the data user holds any of his/her personal data, and to request a copy of such personal data held by that user.

Enforcement

Enforcement:

The PCPD is empowered to investigate into suspected breaches of the PDPO, including summoning individuals to give evidence and inspect personal data systems, (i) upon receiving complaints or (ii) if it has reasonable grounds to believe there may be breaches of the PDPO.

If the PCPD finds breaches of the PDPO in its inquiries, it may issue an "enforcement notice" directing the data user to remedy and prevent recurrences of the breaches.

Fines/Criminal Penalties:

Contravention of an enforcement notice is an offence which could result in (a) a maximum fine of HK$50,000, (b) imprisonment for 2 years, and (c) a daily penalty of HK$1,000.

The PDPO also sets outs a range of specific penalties for violation of certain requirements, including a fine of up to HK$1,000,000 and/or imprisonment for up to 5 years for providing personal data for gain to another person for use by that person in direct marketing without the data subject's consent.

Remedies for Individuals:

Individuals who suffer damages as a result of contravention of any requirements under the PDPO by a data user may sue in court for compensation. The PCPD may grant legal assistance to aggrieved individuals who intend to institute proceedings to seek compensation.

Data Processing

Legal Basis for Processing:

The processing of personal data must:

- fall within the original purpose for which the personal data was collected;
- be done with reasonable belief that the use of the data for a new purpose is "clearly in the interest" of the individual; or
- be done with the individual's consent

Sensitive Personal Data:

Although "Sensitive Personal Data" is not defined under the PDPO, the PCPD has published different Codes of Practice specifying additional requirements when dealing with certain types of personal data, including identity card numbers, other personal identifiers and consumer credit data. In particular, the PCPD has indicated that biometric data are sensitive data and should only be collected when necessary with the consent of the data subject.

Special Rules on Data of a Minor:

If consent is required from a data subject who is under the age of 18 in accordance with DPP 3, a consent from a person with parental responsibility for the minor will suffice.

pwc

Individual Rights

Under the PDPO, individuals have certain rights to their personal data:

- **Right to access:** Yes, request to access must be made within a reasonable time and in a reasonable manner in an intelligible form. Data users must comply with a formal data access request made using the PCPD's prescribed form within forty days.
- **Right to correction:** Yes, individuals may lodge a formal data correction request which must be fulfilled within forty days.
- **Right to restriction/opt out of all or specific processing:** Yes, data users must notify and obtain consent from individuals before using their data in their own direct marketing activities or transferring data to third parties for the third parties' marketing activities.
- **Right to deletion:** No, but a data user should erase personal data which can no longer be used to fulfil and/has already fulfilled the purpose (including any directly related purpose) for which the data were collected unless the retention of such data is in accordance with the statutory requirements or is in the public interest.
- **Right to portability:** No, but personal data provided in a data access request must in the form specified in the request.

Security & Data Breaches

Security Requirements: Data users must take "all practicable steps" to ensure that personal data are protected against unauthorized or accidental access, processing, erasure, loss or use, including the implementation of appropriate contractual measures to protect data transferred to a data processor.

Data Breach Notifications Requirements: There is no statutory breach notification requirement in Hong Kong. However, the PCPD has encouraged voluntary notification of data breaches as soon as practicable after data breach to

- the affected individuals;
- the PCPD;
- other relevant law enforcement agencies and regulators; and
- other relevant parties who may be able to take remedial actions to protect the personal data privacy and interests of the individuals affected (e.g. search engine companies which can remove relevant cached links).

Other Business Obligations

Data Protection Officer: Although there is no legal requirement for data users to appoint a data protection officer in Hong Kong, the Best Practice Guide issued by the PCPD ("**BPG**") recommends data users to appoint a senior executive (or the owner/operator of a very small organization) as the Data Protection Officer to oversee the data users' compliance with the PDPO and publish contact details of the person responsible for handling requests and queries from individual in relation to personal data.

Risk Assessments: It is arguable that the security requirements imply the necessity for risk assessments on personal data held. Nevertheless, the BPG indicates that data users should conduct periodic risk assessments and privacy impact assessment to ensure compliance with the PDPO.

Audits: It is arguable that the security requirements imply the necessity for audit and/or inspection on data processors. The BPG indicates that data users should do so.

Service Providers & Cross-Border Transfers

Service Provider Arrangements: Where a data user engages a data processor to process personal data on the data user's behalf, the data user must adopt contractual or other means to prevent (i) any personal data transferred to the data processor from being kept longer than necessary for processing of the data and (ii) any unauthorized or accidental access, processing, erasure, loss or use.

Cross-Border Data Transfers: The PDPO prohibits transfer of personal data to places outside Hong Kong unless certain conditions are met, one key condition being that the data controller has taken all reasonable precautions and exercised all due diligence to ensure that the personal data concerned is given sufficient protection. However, this section has not been put into operation. General obligations on all data transfers will apply equally to cross-border data transfers.

Data controllers who are registered or located in the Greater Bay Area ("**GBA**") and Hong Kong may use the government issued data transfer agreement (standard contract) for cross-border transfer of personal data. Personal data so transferred to Hong Kong may not be transferred to foreign jurisdictions, such as the US or Singapore.

Localization Requirements: There are no localization requirements (such as governmental consent, approval or registration requirement) in Hong Kong.

To Watch

The Hong Kong government is looking to reform the data protection regulatory regime in Hong Kong by introducing the following amendments:

- mandatory data breach notification and reporting requirements;
- requirement for organizations to formulate a clear data retention policy stipulating a maximum data retention period;
- protective measures on cross-border data transfers;
- direct regulation of data processors;
- conferring more powers to PCPD (such powers to conduct criminal investigation, prosecute and administer administrative fines); and
- increased penalties for breaches of the PDPO.

Let's connect to discuss how we can help:

Martyn Huckerby

Partner, Tiang & Partners (an independent Hong Kong law firm and a member of the PwC network)

+852 2833 4918

martyn.p.huckerby@tiangandpartners.com