DATA PROTECTION
LAWS OF THE WORLD
Hong Kong

Downloaded: 14 December 2019
DATA PROTECTION LAWS OF THE WORLD

HONG KONG

LAW

The Personal Data (Privacy) Ordinance (Cap. 486) (Ordinance) regulates the collection and handling of personal data. The Ordinance has been in force since 1996, but, in 2012/2013 was significantly amended (notably with regard to direct marketing).

DEFINITIONS

Definition of personal data

Personal data is defined in the Ordinance as any data:

- Relating directly or indirectly to a living individual
- From which it is practicable for the identity of the individual to be directly or indirectly ascertained, and
- In a form in which access to or processing of the data is practicable

Definition of sensitive personal data

There is not a separate concept of sensitive personal data in the Ordinance. However, non-binding guidance issued by the Office of the Privacy Commissioner for Personal Data (PCPD) (in the context of biometric data) has indicated that higher standards should be applied as a matter of best practice to more sensitive personal data.

NATIONAL DATA PROTECTION AUTHORITY

The Office of the Privacy Commissioner for Personal Data

12/F, Sunlight Tower
248 Queen's Road East
Wanchai
Hong Kong

T +852 2827 2827
F +852 2877 7026

http://www.pcpd.org.hk/

The PCPD is responsible for overseeing compliance with the Ordinance.

REGISTRATION
Currently, there is no requirement for organizations that control the collection and use of personal data (known as "data users") to register with the data protection authority.

However, under the Ordinance the PCPD has the power to specify certain classes of data users to whom registration and reporting obligations apply. Under the Data User Return Scheme (DURS), data users belonging to the specified classes are required to submit data returns containing prescribed information to the PCPD, which will compile them into a central register accessible by the public. However, at the time of writing, no register has been created to date. The PCPD has proposed to implement the DURS in phases, with the initial phase covering data users from the following sectors and industries:

- The public sector
- Banking, insurance and telecommunications industries, and
- Organizations with a large database of members (eg, customer loyalty schemes)

A public consultation for the DURS by the PCPD was concluded in September 2011. The PCPD had originally planned to implement the DURS in the second half of 2013. However, in January 2014, the PCPD indicated that it planned to put the DURS on hold until the reforms of the European Union (EU) data protection system have been finalized (as the Hong Kong model is broadly based on the same) but no exact time frame for the implementation has been announced. In light of the European Union General Data Protection Regulation 2016/679 (GDPR), which generally eliminated the data processing registration requirements under EU data protection law, it is unclear now whether the PCPD will implement the Hong Kong DURS scheme.

**DATA PROTECTION OFFICERS**

Currently, there is no legal requirement for data users to appoint a data protection officer in Hong Kong. However, in February 2014, the PCPD issued a best practice guide to advocate the development of a privacy management program and encourage data users to appoint or designate a responsible person to oversee the data users’ compliance with the Ordinance. This role may or may not be a full-time job, and there is no specific requirement for a Hong Kong citizen or resident to hold this role. There is no specific enforcement action or penalty if a company does not appoint a data protection officer.

**COLLECTION & PROCESSING**

A data user may collect personal data from a data subject if:

- The personal data is collected for a lawful purpose directly related to a function or activity of the data user
- The collection is necessary for or directly related to that purpose
- The data to be collected is adequate but not excessive, and
- All practical steps have been taken to ensure that the data subject has been informed, on or before collection of the data, of the following:
  - Whether the supply of personal data by the data subject is obligatory or voluntary and, if obligatory, the consequences of not supplying the data
  - The purposes for which the data will be used
  - The persons to whom the data may be transferred
  - The data subject’s right to request for access to and correction of their personal data, and
  - The name or job title, and address, of the individual to whom requests for access or correction should be sent

Separate, additional notice requirements apply to direct marketing (see below).

Data users may only collect, use and transfer personal data for purposes notified to the data subject on collection (see above), unless a limited exemption set out in the Ordinance applies. Any usage or transfer of personal data for new purposes requires the prescribed consent of the data subject.
Data users are also required to take all practicable steps to ensure the accuracy and security of the personal data; to ensure it is not kept longer than necessary for the fulfillment of the purposes for which it is to be used (including any directly related purpose); and to keep and make generally available their policies and practices in relation to personal data.

In October 2018, the PCPD published a “New Ethical Accountability framework.” Under the framework, the PCPD is effectively urging businesses operating in Hong Kong to undertake privacy impact assessments – referred to as “Ethical Data Impact Assessments, which are already required to some extent under a number of other laws, such as China, the Philippines, as well as GDPR.

TRANSFER

Data users may not transfer personal data to third parties (including affiliates) unless the data subject has been informed of the following on or before his / her personal data was collected:

- That his / her personal data may be transferred
- The classes of persons to whom the data may be transferred

There are currently no restrictions on transfer of personal data outside of Hong Kong, as the cross-border transfer restrictions set out in section 33 of the Ordinance were held back and have not yet come into force. A proposal to implement them is under active consideration by the Hong Kong government, but this process has been delayed while consideration is given to recent developments in cross-border data transfers in the EU. If these restrictions come into force as currently drafted, they will have a significant impact upon outsourcing arrangements, intragroup data sharing arrangements, compliance with overseas reporting obligations and other activities that involve cross-border data transfer.

Nevertheless, non-binding best practice guidance published by the PCPD encourages compliance with the cross-border transfer restrictions in section 33 of the Ordinance, which prohibit the transfer of personal data to a place outside Hong Kong unless certain conditions are met (including a white list of jurisdictions; separate and voluntary consent obtained from the data subject; and an enforceable data transfer agreement for which the PCPD provides suggested model clauses).

SECURITY

Data users are required by the Ordinance to take all practical steps to ensure that personal data is protected against unauthorized or accidental access, processing, erasure, loss or use, having regard to factors including the nature of the personal data and the harm that could result if data breaches or leaks were to occur.

Where the data user engages a data processor to process personal data on its behalf, the data user must use contractual or other means to:

- Prevent unauthorized or accidental access, processing, erasure, or loss of use of the personal data, and
- Ensure that the data processor does not retain the personal data for longer than necessary

BREACH NOTIFICATION

Currently there is no mandatory requirement under the Ordinance for data users to notify authorities or data subjects about data breaches in Hong Kong. However, according to non-binding guidance issued by the PCPD, as a matter of best practice the PCPD encourages notification to the PCPD, and to data subjects where there would be a risk of harm by not notifying.

Recent high profile data incidents may lead regulators and politicians to consider introducing more stringent breach notification rules. The PCPD has already hinted at increased use of compliance checks and greater publication of investigation reports as part of “fair” enforcement of the law.

ENFORCEMENT
The PCPD is responsible for enforcing the Ordinance. Generally, unless a specific offense applies, if a data user is found to have contravened the data protection principles of the Ordinance, the PCPD may issue an enforcement notice requiring the data user to take steps to rectify the contravention. Failure to abide to the enforcement notice is a criminal offense, punishable by a fine of up to HK$50,000 and imprisonment for up to two years, as well as a daily penalty of HK$1,000 if the offense continues after conviction. In the case of subsequent convictions, additional and more severe penalties apply. There are also certain specific offenses under the Ordinance which are triggered directly without the intermediary step of an enforcement notice. For example:

- Breach of certain provisions relating to direct marketing is punishable by a fine of up to HK$1 million and imprisonment of up to five years, depending on the nature of the breach, and
- Disclosing personal data of a data subject obtained from a data user without the data user’s consent is an offense punishable by a fine of up to HK$1 million and imprisonment of up to five years, where such disclosure is made with certain intent, or where the disclosure causes psychological harm to the data subject.

Appeals from enforcement decisions of the PCPD may be made to the Administrative Appeals Board.

In addition to criminal sanctions, a data subject who suffers damage by reason of contravention of the Ordinance may also seek compensation from the data user through civil proceedings. The PCPD operates an assistance scheme for data subjects in this regard.

In light of recent high profile data incidents, the PCPD may further strengthen its enforcement against breaches of the Ordinance through more frequent compliance checks and publication of investigation reports. It is also expected that the government, consumer and finance/credit industries are likely to be in the spotlight of enforcement in 2019 in light of those recent data incidents.

**ELECTRONIC MARKETING**

Specific provisions of the Ordinance govern the use and sharing of personal data for the purposes of direct marketing (meaning the offering, or advertising the availability of goods, facilities or services, or the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes), when such marketing is conducted through “direct marketing means” (being the sending of information or goods, addressed to specific persons by name, by mail, fax, electronic mail or other means of communication; or making telephone calls to specific persons).

The direct marketing provisions generally require data users who wish to use personal data for the data user’s own direct marketing purposes to obtain prior consent from the data subject for such action and notify the data subject as follows:

- That the data user intends to use the individual’s personal data for direct marketing
- That the data user may not so use the personal data unless the data subject has received the data subject’s consent to the intended use
- The kind(s) of personal data to be used
- The class(es) of marketing subjects (ie, goods/services to be marketed) in relation to which the data is to be used, and
- The response channel through which the individual may, without charge, communicate the individual’s consent to the intended use

Furthermore, if the consent was given orally, data users have the additional obligation to send a written confirmation to the data subject confirming the particulars of the consent received.

The direct marketing provisions generally require data users who wish to share personal data with a group company or a third party for their direct marketing purposes (eg, for joint marketing, or in connection with a sale of a marketing list) to obtain their prior written consent and to notify the data subject as follows:

- That the data user intends to provide the individual’s personal data to another person for use by that person in direct
marketing

- That the data user may not so provide the data unless the data user has received the individual’s written consent to the intended provision
- That the provision of the personal data is for gain (if it is to be so provided)
- The kind(s) of personal data to be provided
- The class(es) of persons to which the data is to be provided
- The class(es) of marketing subjects (ie, goods/services to be marketed) in relation to which the data is to be used, and
- The response channel through which the individual may, without charge, communicate the individual’s consent to the intended use

When data users use personal data for the purposes of direct marketing for the first time, they must inform the subjects that they may opt out at any time, free of charge. In practice, it is common for most direct marketing email messages in Hong Kong contain unsubscribe functions, not just the first message.

Hong Kong’s anti-spam framework is set out in the Unsolicited Electronic Messages Ordinance (Cap. 593), under which three types of Do-Not-Call (DNC) registers are maintained, namely the DNC for fax, short messages and pre-recorded telephone messages. Person-to-person telemarketing calls are not regulated by this framework.

In 2018, the Hong Kong government proposed that a statutory DNC register be set up allowing individuals who do not wish to receive person-to-person calls to register their phone numbers with the register, which shall be administered by the PCPD. The legislative proposal to implement the new DNC is being prepared by the Hong Kong government.

ONLINE PRIVACY

The principles as stated in the Ordinance also apply in the online environment. For example, under the Ordinance, data users have the obligation to inform data subjects of the purposes for collecting their personal data, even if personal data is collected through the Internet. If a website uses cookies to collect personal data from its visitors, this should be made known to them. Data users should also inform the visitors whether and how non-acceptance of the cookies will affect the functionality of the website.

KEY CONTACTS

Scott Thiel
Partner & Co-Chair of Asia-Pac Data Protection and Privacy Group
T +852 2103 0519
scott.thiel@dlapiper.com

Carolyn Bigg
Of Counsel
T +852 2103 0576
carolyn.bigg@dlapiper.com

DATA PRIVACY TOOL
You may also be interested in our Data Privacy Scorebox to assess your organization’s level of data protection maturity.
Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.