DATA PROTECTION LAWS OF THE WORLD

Hong Kong, SAR

DLA PIPER

HONG KONG, SAR

Last modified 11 January 2024

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). The Personal Data (Privacy) (Amendment) Ordinance (**Amendment Ordinance**) came into force in October 2021 and introduced new offences of doxxing and corresponding penalties.

At Bill stage, the Amendment Ordinance had originally included a number of other proposed amendments to the Ordinance (as per the January 2020 Consultation Paper), e.g. introducing a mandatory data breach notification mechanism, requiring data users to formulate a data retention policy, empowering the Office of the Privacy Commissioner for Personal Data (**PCPD**) to impose administrative fines linked to annual turnover and regulating data processors directly. According to its report to the Legislative Council in February 2023 (PCPD’s Report), the PCPD is studying further amendments to the Ordinance with the Hong Kong Government to strengthen personal data protection and address challenges including those posed by the internet technology developments.

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.

The January 2020 Consultation Paper proposed to expand the definition of personal data to cover anonymized information where the relevant individual can be re‑identified.

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 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 (PCPD)

Unit 1303, 13/F, Dah Sing Financial Centre
248 Queen's Road East

Wanchai
Hong Kong

Telephone

+852 2827 2827

Fax

+852 2877 7026

Website

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 (e.g. 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, the PCPD issued a best practice guide in February 2014 (which was further revised in March 2019) 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. 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" (which is akin to a "data controller" under GDPR) 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 rights 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.

Separately, 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 fulfilment of the purposes for which it is to be used (including any directly related purposes); and to keep and make generally available their policies and practices in relation to personal data.

While the Ordinance currently does not regulate data processors, this was proposed in the January 2020 Consultation Paper and also referred to as an amendment direction in the PCPD’s Report issued in February 2023.

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. In August 2021, the PCPD published the Guidance on the Ethical Development and Use of Artificial Intelligence with the aim to help organizations manage the privacy and ethical risks associated with development and use of Artificial Intelligence.

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 their personal data was collected:

- that their personal data may be transferred; and
- 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 section 33 (perhaps with amendments) was put forward to the Hong Kong Government in 2015, but this process has been delayed. Notably, however, these were not included in the January 2020 Consultation Paper or mentioned in the PCPD’s Report issued in February 2023. 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). In practice, most data users will enter into data transfer agreements by putting in place the recommended model contractual clauses for cross‑border transfer of personal data published by the PCPD (RMCs) with the overseas recipient prior to conducting any overseas transfers activities.

On 13 December 2023, the Standard Contract for the Cross-boundary Flow of Personal Information within the Guangdong-Hong Kong-Macao Greater Bay Area (Mainland, Hong Kong) (GBA) (GBA Standard Contract) and the implementation guidelines were

announced to promote the safe and orderly cross-boundary flow of personal data within the GBA. Adoption of GBA Standard Contract is on a voluntary basis. The PCPD published guidance in December 2023 to help organizations in Hong Kong understand the applicability of the GBA Standard Contract and its relationship with the RMCs.

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.

The January 2020 Consultation Paper proposed to require organizations to formulate and publish a clear data retention policy specifying retention period(s) for personal data collected. The PCPD’s Report issued in February 2023 also referred to this as an amendment direction.

BREACH NOTIFICATION

There is no statutory definition of a data breach under the Ordinance. However, under the non–binding guidance issued by the PCPD, data breach is defined as a “*suspected breach of data security of personal data held by a data user, exposing the data to the risk of unauthorized or accidental access, processing, erasure, loss or use*.”

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 (last updated in June 2023), as a matter of best practice the PCPD encourages notification to the PCPD and to the affected data subjects as soon as practicable after becoming aware of the data breach, particularly if the data breach is likely to result in a real risk of harm to affected data subjects. Specifically, the non‑binding guidance recommends that organizations should follow the following key steps in order when handling a data breach:

- immediate gathering of essential information;
- containing the data breach;
- assessing the risk of harm;
- considering giving data breach notifications; and
- documenting the breach.

To assist organizations in reporting data breach incidents to the PCPD more effectively and in a more convenient manner, the PCPD provides an e-Data Breach Notification Form on its website.

Past high profile data incidents in recent years have led 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. The January 2020 Consultation Paper proposed mandatory breach notification requirement for organizations to notify a data incident to both the PCPD and the impacted data subjects within the prescribed period where there is a real risk of significant harm. The PCPD’s Report issued in February 2023 also indicated that establishing a mandatory data breach notification mechanism would be one of the upcoming amendments.

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 by 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 high profile data incidents in recent years, the PCPD may further strengthen its enforcement against breaches of the Ordinance through more frequent compliance checks and publication of investigation reports, as well as increased co‑ operation with local and international authorities.

The January 2020 Consultation Paper proposed to confer additional powers on the PCPD to impose administrative fines linked to the annual turnover of the organization, which would, if implemented, result in a significant increase in financial penalties at a much higher amount calculated by reference to annual turnover. The PCPD’s Report issued in February 2023 also mentioned empowering the PCPD to impose administrative fines linked to annual turnover as an amendment direction.

Doxxing

Under the Amendment Ordinance it is an offence to disclose, without the data subject’s consent, any personal data with an intent to cause harm to the data subject or any family member of the data subject.

Depending on the severity of the offence, any person who commits the offence is punishable on conviction with:

- a fine at level 6 (i.e. HK$100,000) and to imprisonment for 2 years; or
- a fine of HK$1,000,000 and to imprisonment for 5 years if the disclosure causes harm to the data subject or any family member of the data subject.

The PCPD is also empowered to conduct criminal investigations and commence prosecution for doxxing offences. Among other things:

- The PCPD is granted wide powers under the Amendment Ordinance to access documents and information from any person, or require any person to answer questions or provide relevant materials to facilitate an investigation in relation to doxxing offences.
- The PCPD may also, with a warrant, enter premises and seize any materials or devices in the premises which may be relevant to the investigation as well as decrypt any material stored in these devices.

As the anti‑doxxing provisions have extra‑territorial effect, the PCPD is empowered to serve cessation notices to operators of electronic platforms including websites and online applications (regardless of whether these operators are based in Hong Kong or outside Hong Kong) where personal data has been disclosed without the individual's consent. The cessation notices will require the recipient of the notice to take steps to remove the doxxing content or restrict the disclosure of personal data which has been made.

Failure to comply with the cessation notice is an offence. Persons contravening the offence will be liable, on first conviction, to a fine at level 5 (i.e. at HK$ 50,000) and to imprisonment for two years.

Since the Amendment Ordinance came into force to the end of 31 October 2023, the PCPD commenced 228 criminal investigations and arrested 40 persons in 39 cases among which 13 persons were charged with doxing offences and 11 of them being convicted. The longest imprisonment sentence was eight months. The PCPD also referred 55 cases to the Hong Kong

Police Force in respect of the more serious cases and cases involving other criminal offences. In addition, the PCPD issued over 1,800 cessation notices to 41 online platforms, requesting the removal of nearly 27,000 doxxing messages with a compliance rate of over 95% and over 180 doxxing channels being removed.

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 (i.e. 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 direct marketing purposes (e.g. 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 (i.e. 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 subsequent direct marketing communications in Hong Kong to contain unsubscribe functions, not just in 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 2019, a legislative proposal was published to implement the new DNC to provide an "opt out" framework to permit recipients to request to stop receiving person‑to‑person telemarketing calls. At the time of writing, the relevant bill is not yet announced.

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.

With the coming into effect of the Amendment Ordinance, anti‑doxxing law is now in force in Hong Kong. It is an offence to disclose any personal data without the data subject's consent with an intent to cause harm to the data subject or any family member of the data subject.

KEY CONTACTS

Carolyn Bigg
Partner, Global Co-Chair of Data Protection, Privacy and Security Group
T +852 2103 0576
carolyn.bigg@dlapiper.com

Venus Cheung
Registered Foreign Lawyer
T +852 2103 0572
venus.cheung@dlapiper.com

Angele Lok
Associate
T +852 2103 0677
angele.lok@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.