Data Privacy Law

The Personal Data (Privacy) Ordinance

The Personal Data (Privacy) Ordinance (the "PDPO") was passed in 1995 and took effect from December 1996 (except certain provisions). It is one of Asia's longest standing comprehensive data protection laws. It has its origins in the August 1994 Law Reform Commission Report entitled "Reform of the Law Relating to the Protection of Personal Data"[1], which recommended that Hong Kong introduce a new privacy law based on the OECD Privacy Guidelines 1980[2] to ensure an adequate level of data protection to retain its status as an international trading centre and give effect to human rights treaty obligations. The PDPO underwent major amendments in 2012, the most significant of which being the introduction of direct marketing provisions and other additional protection to cope with new privacy challenges and address public concerns.

Click here to view The Personal Data (Privacy) Ordinance

The Ordinance at a Glance

The PDPO is applicable to both the private and the public sectors. It is technology-neutral and principle-based. The Data Protection Principles ("DPPs" or "DPP", which are contained in Schedule 1 to the PDPO, outline how data users should collect, handle and use personal data, complemented by other provisions imposing further compliance requirements.

Before going into the details of the compliance requirements, it is important to first get familiar with a few key definitions under the PDPO:

Personal Data means information which relates to a living individual and can be used to identify that individual. It must also exist in a form which access to or processing of is practicable.

Data Subject is the individual who is the subject of the personal data.

Data User is a person who, either alone or jointly with other persons, controls the collection, holding, processing or use of personal data.

Data Processor is a person who processes personal data on behalf of another person (a data user), instead of for his/her own purpose(s). Data processors are not directly regulated under the PDPO. Instead, data users are required to, by contractual or other means, ensure that their data processors meet the applicable requirements of the PDPO.

The collective objective of DPPs is to ensure that personal data is collected on a fully-informed basis and in a fair manner, with due consideration towards minimising the amount of personal data collected. Once collected, the personal data should be processed in a secure manner and should only be kept for as long as necessary for the fulfillment of the purposes of using the data. Use of the data should be limited to or related to the original collection purpose. Data subjects are given the right to access and make correction to their data.

DPP1 Purpose and Manner of Collection

DPP1 provides that personal data shall only be collected for a lawful purpose directly related to a function or activity of the data user. The data collected should be necessary and adequate but not excessive for such purpose. The means of collection should be lawful and fair.

If you collect personal data from data subjects directly, you should inform the data subjects whether it is obligatory or voluntary to supply the data, the purpose of using their data and the classes of person to whom their data may be transferred. You should also inform them of the right and means to request access to and correction of their data.

DPP2 Accuracy and Duration of Retention

DPP2 requires data users to take all practicable steps to ensure that personal data is accurate and is not kept longer than is necessary for the fulfillment of the purpose for which the data is used. If you engage a data processor for handling personal data of other persons, you should adopt contractual or other means to ensure that the data processor comply with the mentioned retention requirement.

Section 26 of PDPO requires data users to take all practicable steps to erase personal data that is no longer required for the purpose for which the data is used, unless erasure is prohibited by law or is not in the public interest. Section 26 could be engaged when a data user fails to respond to a complaint or request from a data subject for erasure of personal data. This situation attracts a heavier criminal gravity than just keeping the data longer than is necessary under DPP2. Contravention of the requirement under section 26 is an offence, punishable by a fine of up to HK$10,000.

DPP3 Use of Data

DPP3 prohibits the use of personal data for any new purpose which is not or is unrelated to the original purpose when collecting the data, unless with the data subject's express and voluntary consent. A data subject can withdraw his/her consent previously given by written notice.

Regarding restrictions on use of personal data, Part 6A of the PDPO further requires that data users must obtain informed consent before using a data subject's personal data for direct marketing or transferring the data to a third party for direct marketing. The consent must be an explicit indication by the data subject and broadly covers an indication of no objection. In other words, silence cannot constitute consent.

Besides, the consent must be an informed one. The data user must inform the data subject of the intention to use his/her personal data for direct marketing, the fact that the data user cannot so use the data unless with consent of the data subject, the kinds of personal data to be used, the classes of marketing subjects to be involved. The data user must also notify the data subject of the right to opt out. If the data user intends to transfer the data to a third party for direct marketing, he/she should inform the data subject of such intention, the classes of transferees, the classes of marketing subjects to be involved and the fact that the transfer is for a gain, etc. Failure to comply with the direct marketing requirements is an offence and can result in a fine of $500,000 and imprisonment for 3 years, or up to a fine of $1,000,000 and imprisonment for 5 years if data was provided to a third party for gain.

There is another noteworthy offence in section 64 of the PDPO regarding disclosure by a person of personal data of a data subject obtained from a data user without the data user's consent. To constitute this offence, either the disclosing person has an intent to obtain gain or cause loss to the data subject or the disclosure causes psychological harm to the data subject. Although this kind of acts may be already covered under DPP3 (restriction against using personal data for a new purpose), this section was enacted to make it an offence due to the seriousness of the privacy intrusion and gravity of harm that may be caused to data subjects arising from such kind of acts. The maximum penalty is a fine of $1,000,000 and imprisonment for 5 years.

DPP4 Data Security

DPP4 requires that data users take all practicable steps to protect the personal data they hold against unauthorised or accidental access, processing, erasure, loss or use. Data users should have particular regard to the nature of the data, the potential harm if those events happen, measures taken for ensuring the integrity, prudence and competence of persons having access to the data, etc. If you engage a data processor to process the personal data held, you must adopt contractual or other means to ensure that the data processor comply with the mentioned data security requirement.

DPP5 Openness and Transparency

DPP5 obliges data users to take all practicable steps to ensure openness of their personal data policies and practices, the kind of personal data held and the main purposes for holding it.

DPP 6 Access and Correction

DPP6 provides data subjects with the right to request access to and correction of their own personal data. A data user should give reasons when refusing a data subject's request to access to or correction of his/her personal data.

DPP6 is supplemented by detailed provisions in Part 5 of the PDPO which cover the manner and timeframe for compliance with data access requests and data correction requests, the circumstances in which a data user may refuse such requests, etc. Data users are also required to maintain a log book to record all refusals made.

Exemptions

While data privacy is an important right, the interests protected under PDPO have to be balanced against other important rights or public interest. PDPO provides a number of exemptions from some compliance requirements under particular circumstances. Examples include crime prevention or prosecution, security and defence, statistics and research, news activity, protecting a data subject's health etc. There is also an exemption if 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. A table summarising the exemption provisions can be found here.

An exemption is a defence for a data user to avoid liability when he/she fails to comply with certain compliance requirements under PDPO. As a data user, you should not routinely rely on exemptions. Instead, you should consider them on a case-by-case basis and you have to prove that an exemption applies in your case to defend a contravention of PDPO. On the other hand, the fact that a data user can rely on an exemption does not impose an obligation upon him/her to rely on such exemption. Nor does it empower any other person to compel the data user to rely on such exemption.

Enforcement

The Office of the Privacy Commissioner for Personal Data ("the Commissioner") was established under PDPO as the dedicated data privacy regulator. If you find a possible breach of PDPO by a particular data user in relation to the handling of your personal data, you may lodge a complaint with the Commissioner. Depending on the facts involved and the evidence available, the Commissioner may carry out, refuse to carry out or terminate an investigation of the complaint.

When the Commissioner receives a complaint or has reasonable grounds to believe there may be a contravention of PDPO, the Commissioner may conduct an investigation of the suspected contravention and publish a report setting out the investigation results and recommendations if it is in the public interest to do so. If, upon completion of an investigation, it is found that the relevant data user is contravening or has contravened PDPO, the Commissioner may issue an enforcement notice to the data user directing remedial and/or preventive steps to be taken.

Contravention of a DPP is not an offence. However, contravention of certain provisions of PDPO is an offence. Examples include section 26 regarding erasure of personal data that is no longer required for the purpose for which it is used, section 64 regarding disclosure of personal data obtained from a data user without the data user's consent and the direct marketing provisions, etc..

Contravention of an enforcement notice issued by the Commissioner is also an offence which may result in a maximum fine of $50,000 and imprisonment for 2 years, with a daily penalty of $1,000. Subsequent convictions can result in a maximum fine of $100,000 and imprisonment for 2 years, with a daily penalty of $2,000. A table summarising the various offences under PDPO and the respective penalties can be found here.

Data subjects may also seek compensation by civil action from data users for damage caused by a contravention of the PDPO. The Commissioner may provide legal assistance to the aggrieved data subjects if the Commissioner thinks fit to do so.

In addition, the Commissioner may proactively carry out an inspection of a personal data system of a data user or a class of data users for the purpose of making recommendations on how compliance may be enhanced by the data user(s). The Commissioner is also empowered to issue codes of practices to provide practical guidance on how to comply with the requirements under PDPO. Non-compliance with a code of practice itself is not an offence but can be a proof of contravention of the relevant requirement under PDPO.

Other Statutory Responsibilities

The Commissioner also has other responsibilities to promote public awareness and understanding of PDPO, examine proposed legislation with impact on data privacy, undertake research and monitor development in information technology that may affect personal data protection, etc. In addition to the role of an enforcer, the Commissioner also serves as an educator in promoting public understanding of PDPO and a facilitator in engaging with organisations to advocate the inclusion of personal data privacy protection in their businesses' practices and operation in Hong Kong.

[1] *The Law Reform Commission also adverted to the then draft version of Directive 95/46/EC of the European Parliament and of the Council.*

[2] *"OCED Privacy Guidelines 1980" is a common name for the original 1980 version of the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data".*