GETTING THE DEAL THROUGH

Data Protection & Privacy 2015

Contributing editor

Rosemary P Jay

Hunton & Williams

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Business development managers
George Ingledew
george.ingledew@lbresearch.com

Alan Lee
alan.lee@lbresearch.com

Dan White
dan.white@lbresearch.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 7908 1188
Fax: +44 20 7229 6910

First published 2012
Third edition
ISSN 2051-1280

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Hong Kong

Chloe Lee
J S Gale & Co

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

Personal Data (Privacy) Ordinance (Cap 486) (the Ordinance) is the primary legislation regulating the protection of PII in Hong Kong. The Ordinance is based on the relevant treaty provisions of the International Covenant of Civil and Political Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Directive 95/46/EC also prompted the enactment of the Ordinance.

Schedule 1 to the Ordinance contains the six data protection principles (DPP), which are the core provisions.

Personal Data (Privacy) (Amendment) Ordinance (the Amendment Ordinance) was enacted in 2012 to make various amendments to the Ordinance. The purpose is to enhance the protection of personal data privacy of individuals.

The Ordinance is regulating the 'data user', ie, 'a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data'.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the powers of the authority.

The Privacy Commissioner for Personal Data (Commissioner) is responsible for overseeing personal data protection law.

The Commissioner has various powers and duties, including:

- overseeing the administration and supervision of the Commissioner's office;
- formulating operational policies and procedures to implement the provisions of the Ordinance;
- monitoring and supervising compliance with the provisions of the Ordinance;
- exercising powers to approve and issue codes of practice providing practical guidance for compliance with the provisions of the Ordinance;
- promoting awareness and understanding of, and compliance with, the provisions of the Ordinance;
- examining any proposed legislation (including subsidiary legislation) that the Commissioner considers may affect the privacy of individuals in relation to personal data and report the results of the examination to the persons proposing the legislation;
- carrying out inspections of personal data systems including those of Government departments and statutory corporations;
- investigating, upon receipt of complaints from data subjects or on his own initiative, suspected breaches of requirements of the Ordinance;
- undertaking research into, and monitoring developments in, the processing of data and computer technology that may have adverse effects on the privacy of individuals in relation to personal data; and
- liaising and cooperating with persons performing similar data protection functions in any place outside Hong Kong in respect of matters of mutual interest concerning the privacy of individuals in relation to personal data.

3 Breaches of data protection

Can breaches of data protection lead to criminal penalties? How would such breaches be handled?

A breach of any provision of the Ordinance or an enforcement notice issued by the Commissioner could be criminally sanctioned but a breach of the DPP itself is not an offence (sections 64 and 64A, Ordinance). For example, it is a criminal offence to obstruct, hinder or resist the Commissioner's investigation and an offender is punishable by a fine of up to HK$10,000 (approximately US$1,300) and/or imprisonment up to six months.

A breach of an enforcement notice is a criminal offence and attracts a fine of up to HK$50,000 plus a daily fine of up to HK$1,000 for a continuing breach and imprisonment up to two years. If a data user initially complied but later intentionally committed any act or omission in contravention of the requirement in the enforcement notice, it is also a criminal offence which attracts the same penalty.

A repeat offender can face the penalty doubled.

In case of a breach, the Commissioner may investigate, issue an enforcement notice if a breach is found after investigation and/or publish an investigation report, if the Commissioner considers that the public interest requires such publication.

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The Ordinance applies in both the public and the private sectors. Any person, whether natural or legal such as a company or public entity, who controls the collection, holding, processing or use of personal data is subject to the Ordinance.

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

The Interception of Communications and Surveillance Ordinance regulates the conduct of the interception of communications and the use of surveillance devices by, or on behalf of, public officers and to provide for related matters. The data protection law does not apply to the collection, holding, processing or use of personal data in the context of any interception or surveillance made under prescribed authorisation including a judge's authorisation, an executive authorisation or an emergency authorisation.

The Amendment Ordinance regulates the use of personal data for direct marketing. In addition, the Unsolicited Electronic Message

Ordinance also regulates the sending of spam electronic marketing and specifically, the choice to opt out of receiving the communications must be provided to the recipients.

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas?

There are 'soft law' instruments, for example the Code of Practice on Consumer Credit Data, the Code of Practice on Human Resource Management and the Code of Practice on the Identity Card Number & Other Personal Identifiers that are applicable to the specific areas.

7 PII formats

What forms of PII are covered by the law?

The Ordinance covers all accessible data relating to an identifiable individual, ie, 'personal data' that are contained in any recording medium. 'Data' is defined widely as 'any representation of information (including an expression of opinion) in any document, and includes a personal identifier'. 'Document' could be in paper or electronic format. However, oral conversation or comment is excluded from the Ordinance.

'Personal data' must relate either directly or indirectly to a living individual, be reasonably retrievable and allow the individual to be ascertained from those data.

8 Extraterritoriality

Is the reach of the law limited to data owners and data processors established or operating in the jurisdiction?

It does not matter where the collection or processing of the data occurs if the data are controlled by a data user in Hong Kong. Controlling of one aspect of the data cycle is sufficient to make the activity fall within the Ordinance.

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide services to owners?

Generally, all processing or use of personal data is covered by the Ordinance but a third party processor who holds, processes or uses the personal data solely on behalf of the data user and not for any of his own purposes will not be bound by the DPPs or the Ordinance.

Legitimate processing of PII

10 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

A data user could only collect personal data if it is done lawfully and the data is necessary for a lawful purpose directly related to a function or activity of the data user. The data user must inform the individual whether it is obligatory or voluntary that he or she supply the data (and if obligatory, the consequences of not supplying), the purpose for which the data are to be used and the classes of persons to whom the data may be transferred.

11 Legitimate processing – types of data

Does the law impose more stringent rules for specific types of data?

There is no special rule regarding 'sensitive' type of data.

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose data they hold? What must the notice contain and when must it be provided?

At the time of collection, a data user must inform the 'data subject', ie, an individual to whom the personal data relate of the purpose for which the data are to be used, the classes of persons to whom data will be transferred, whether giving personal data is obligatory or voluntary and the consequences of not providing data.

A data user is also required to notify data subjects of their rights to access and correct the personal data and contact details of the officer handling access and correction requests.

A data user is also required to make its data policy and practice generally available, stating the types of personal data held and their main purposes. The provision of the information could be through a notice-board or on the website of the data user.

There are some new provisions specifically applicable to 'direct marketing', ie, advertising or soliciting addressed to specific persons directly. A data user must inform the data subject of information prescribed under the law including the kinds of data to be used for direct marketing, the classes of marketing subjects (ie, the kinds of services and products which may be marketed for which the data will be used) and provide a channel for the data subject to object to the intended use or provision of personal data (ie, the 'opt-out' right) in an easy-to-read and understandable format. If the data user intends to use the data for his or her own purposes, he or she could inform the data subject either orally or in writing. Data users, after receiving oral consent, should send a written confirmation to the data subject to confirm the date of receipt of the consent together with the kinds of personal data and classes of goods or services covered by the consent within 14 days. If data are given to another data user, the information must be given in writing no matter whether the provision is for gain or not. Furthermore, if a data user intends to provide personal data to others for use in direct marketing, he or she could only do so after the data subject consents or does not object to the provision.

13 Exemption from notification

When is notice not required?

The Ordinance provides for a broad exemption for personal data held for domestic or recreational purposes. It also exempts for public or social interests the application of the data privacy notice requirement in the context of judicial functions and emergency situations concerning individuals in life-threatening situations.

There are also exemptions for data users from the requirements to grant access to individuals to their PII and to limit the use of PII to the original purpose at the time of the collection of information in order to protect the public interest in such matters as security, defence, prevention or detection of crime, assessment or collection of tax, news activities and health. Furthermore for employment-related records, there are certain limited exemptions from the requirement to comply with access requests from individuals.

In the case of direct marketing, a data user does not need to notify the data subject of his intention to use personal data in direct marketing if such personal data had been used by the data user for direct marketing before 1 April 2013. This is called the 'grandfathering arrangement'.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The consent of an individual must be obtained for the use of his or her personal data beyond the purpose for which collection was made or a directly related purpose. And in case of direct marketing, individuals do have the right to object to the use or provision of their personal data for the use of direct marketing. Other than these, individuals' choice or control over their personal data is confined to knowing about the kinds of data being held and the purposes for which the data are used, to access, get a copy and request correction of their data, and to be compensated for damage including injury to feelings arising from a breach of the Ordinance. However, enforcing the compensation right is a rare occurrence.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

A data user must take all practical steps to ensure that personal data are accurate and transmit any corrections made to previous data users

who supplied the incorrect data. A data user must respond to correction requests made by data subjects or failure will constitute an offence.

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

A data user can collect only adequate but not excessive data. A data user must take all practicable steps to erase personal data if the keeping of data is no longer necessary for the purpose for which the data was used including any directly related purpose.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

The Ordinance restricts the use of data to the purpose specified at the time of the collection of the data or a directly related purpose. The finality principle applies.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The finality principle will not apply if there is consent from a data subject. Consent from a data subject must be express and given voluntarily. Therefore, consent could not be implied or inferred. Further, consent must be reasonably specific to avoid giving blanket consent rendering restriction meaningless.

There are other exemptions specifically provided in the Ordinance covering judicial functions, employment staff planning, processing for employment, appointment, promotion, academic or contract award, safeguarding security or defence or international relations of Hong Kong, prevention or detection of crime, health relating to physical or mental health of individuals, legal proceedings privilege, news activity, statistics and research, business due diligence exercise, emergency situations concerning individuals in life-threatening situations and government record preservation.

Security

19 Security obligations

What security obligations are imposed on data owners and entities that process PII on their behalf?

Data users are required to take all reasonably practical steps to protect personal data against any unauthorised or accidental access. Data users should classify the data they are holding according to the sensitivity. There should be an assessment of the potential security risks and corresponding protective measures are required. Even data that are not reasonably practicable to be retrieved or processed are included in this principle to prevent data from going to someone who could use them in a way harmful to the data subject.

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

20 Notification of security breach

Does the law include obligations to notify the regulator or individuals of breaches of security?

There is no obligation on the data users to notify the Commissioner or data subjects of breaches of security. Yet according to a guidance issued by the Commissioner, it is advisable that a data user does notify the data subjects and the relevant parties when real risk of harm is reasonably foreseeable. The data user should consider the circumstances of the case and decide whether to notify any of the parties including the affected data subjects, the Commissioner and law enforcement agencies.

The notification should include information such as a general description of what occurred, the date and time of the breach together with the duration, the list of the types of personal data involved and an assessment of the risk of harm as a result of the breach.

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

It is not mandatory but highly recommendable to appoint a data protection officer.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

Data users are required to keep and maintain a 'log book'.

There are four types of information that must be entered in the log book:

- particulars of the reasons for refusing to comply with a data access request;
- particulars of the prejudice that would be caused to the interest protected by the exemption concerned, if the existence or non-existence of the personal data to which the data access request concerned was disclosed;
- particulars of the reasons for refusing to comply with a data correction request; and
- any other particulars required by regulations made under the Ordinance. There are no such regulations at present.

Data users are required to allow and assist the inspection and copying of the log book by the Commissioner at any reasonable time.

Registration and notification

23 Registration

Are owners and processors of PII required to register with the supervisory authority? Are there any exemptions?

At present, data users are not required to register but the Commissioner is empowered under the Ordinance to specify a class of data users to submit returns with prescribed information for showing their compliance with the data privacy requirements. If implementing such a data user return scheme, the Commissioner will keep and maintain a register of data users who have submitted the returns. The latest development in early 2014 shows that the Commissioner will not roll out the data user return scheme in the near future, and for further details, see the Updates and trends section.

24 Formalities

What are the formalities for registration?

A data user may be required, by serving notice in writing, to submit information to the Commissioner. On the notice, the Commissioner will prescribe what information is needed.

25 Penalties

What are the penalties for a data owner or processor for failure to make or maintain an entry on the register?

Not applicable at present.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

Not applicable at present.

27 Public access

Is the register publicly available? How can it be accessed?

Not applicable at present.

28 Effect of registration

Does an entry on the register have any specific legal effect?

Not applicable at present.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

'Data processor' is defined as a person who processes personal data on behalf of a data user and does not process the data for its own purposes.

If a data user wishes to engage a data processor to process data on his or her behalf, he or she has to adopt contractual or other means to prevent any personal data being kept for longer than necessary for processing the data and to ensure security measures have been properly applied.

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Apart from the general data privacy requirements, there is no specific restriction on the disclosure of personal data to other recipients.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Section 33 of the Ordinance regulates the transfer of personal data to places outside Hong Kong except in specified circumstances. The provision has not yet been implemented since its enactment in 1995.

Section 33 states that data users cannot transfer personal data to a place outside Hong Kong unless they have taken all reasonable precautions and exercised all due diligence to ensure that personal data would be given similar protection to that in Hong Kong. Data users can do so by entering into a contract or other acceptable agreement with the other party to whom the data will be transferred. Alternatively, consent in writing from data subject is required.

Currently, DPPs also govern the transfer of personal data outside Hong Kong. Data users have to adopt contractual or other means to prevent personal data being kept longer than necessary and to ensure they can only be used for the purpose for which the data were originally collected. Contravention of the provisions would not be an offence.

The Commissioner has provided a model contract for this purpose: www.pcpd.org.hk/english/publications/fact1_model.html.

32 Notification of transfer

Does transfer of PII require notification to or authorisation from a supervisory authority?

Data users do not need to notify or seek authorisation from the Commissioner.

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

If overseas service providers make any onward transfer, the data user who originally transferred the data to the overseas service providers may become responsible. The Ordinance provides that any acts of the overseas transferee for the data are regarded as the acts of the Hong Kong data transferor who is liable for any acts that breach our data privacy law.

Rights of individuals

34 Access

Do individuals have the right to see a copy of their personal information held by PII owners? Describe any limitations to this right.

A data user is required to respond to a data access request in writing within 40 days irrespective whether he is holding such data.

There are limitations to the right. A data subject would not be able to access his or her personal data on various grounds including, for instance, the non-disclosure or secrecy requirements in other ordinances.

35 Other rights

Do individuals have other substantive rights?

The Ordinance states that data subjects could request access to personal data for correction. This right is to enable the data subject to monitor the compliance of the data user with the DPPs. The data quality would also be enhanced as the data subject is in the best position to provide accurate and updated data.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals could claim monetary compensation if they suffer damage as a result of breaches of the law. There is no restriction on the amount of damages sought. Injury to feelings would be sufficient.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Rights of individuals are exercisable through both the Commissioner's Office and the judicial system.

As an alternative or in additional to seeking redress from the Commissioner by making a complaint, individuals could start a civil proceeding to claim damages in the judicial system.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

Exemptions include:

- a court, a magistrate or a judicial officer in the course of performing judicial functions is exempted from the DPPs and the provisions on data user returns and register of data users, access to and correction of personal data, inspection of personal data systems and investigations initiated by the Commissioner;
- if disclosure or transfer of personal data would prevent causing serious harm to the physical or mental health of the data subject or any other individual;
- minor's personal data transferred or disclosed by the Hong Kong Police Force or the Customs and Excise Department to the minor's parent or guardian provided that the provision of data would be in the interest of the minor and facilitate the parent or guardian exercising proper care and guardianship of the minor;
- personal data in relation to conducting due diligence in the course of a business merger, acquisition or transfer of business;
- the use of the data that is required or authorised by or under law, by court orders, or in connection with any legal proceedings in Hong Kong or for establishing, exercising or defending legal rights in Hong Kong;
- records that are only used by the Government Records Service solely for the purpose of appraising the records to decide whether they are to be preserved, or for organising and preserving the records;
- the use of personal data to facilitate the process of identification in a life-threatening situation, informing the immediate family members of the situation of an individual and carrying out of emergency rescue or relief services; and
- if the data user could be self-incriminated for any offence other than offences created under the Ordinance by disclosing information.

Update and trends

Since the enactment of the Amendment Ordinance, there has been a 30 per cent increase on the complaints to the Privacy Commissioner relating to the new provisions on direct marketing. The Privacy Commissioner had, in total, referred 20 cases to the Secretary of Justice. This was 33 per cent more than 2012.

A Legal Assistance Scheme was introduced recently to grant legal assistance to those who are aggrieved and want to seek compensation from a data user for harm suffered in relation to a breach of statutory requirements under the Ordinance. Assistance can be in the form of giving legal advice, arranging mediation and providing legal representation. This scheme may enable individuals who would otherwise not be able to pursue action due to lack of resource or knowledge.

Considering the sceptical response of data users and the latest development in the EU's data privacy regime, the Commissioner will promote a voluntary compliance via the Privacy Management Programme instead of rolling out the data user return scheme. The data users are encouraged to embrace personal data protection as part of their corporate governance responsibilities instead of a pure legal compliance issue. Organisational commitment, programme controls and documentation of a formulated personal data policy with periodical employee education and continuing review, etc, are all recommended under the Programme.

The Commissioner is also keen to commence section 33 of the Ordinance to regulate cross-border flows of personal data. A survey of 50 jurisdictions on their personal data protection law and practice was made in 2013 and the Commissioner has provided the government with a proposed white list of jurisdictions having personal data protection comparable to that in Hong Kong. We may expect formal announcement of the commencement date for section 33 at any time.

Supervision

39 Judicial review

Can data owners appeal against orders of the supervisory authority to the courts?

Data users could appeal to the Administrative Appeals Board under the powers given by the Administrative Appeals Board Ordinance. The case could also be further appealed to the Court of Appeal which could make a binding order overriding the Administrative Appeals Board.

40 Criminal sanctions

In what circumstances can owners of PII be subject to criminal sanctions?

There are a few criminal offences created under the Ordinance:

- failure to notify a data subject of his opt-out right in direct marketing for the first time;
- failure to cease using or transferring personal information as requested;
- disclosure of personal data without consent from the data subject with an intent to gain or cause loss to the data subject;
- unauthorised disclosure causing psychological harm to the data subject;
- intentionally repeated contravention of the statutory requirements;
- non-compliance with an enforcement notice;
- failure to comply with the Privacy Commissioner's request to submit or accurately submit a notice for the keeping and maintaining of the register of data users;
- failure to comply with the Privacy Commissioner's verification and correction request regarding user data return;
- failure to correct data upon request;
- failure to supply accurate information when trying to obtain the Privacy Commissioner's consent to carry out a matching procedure;
- failure to return and destroy personal data after the completion of a due diligence exercise; and
- any contraventions of requirements under the Ordinance.

41 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

Cookies or online behavioural tracking data will be deemed to be personal data if they contain information that allows the identification of an individual directly or indirectly. The cookie or online behavioural tracking itself is not personal data.

The Commissioner recommends that a data user should state clearly the kind of information cookies will collect, who will the data be transferred to and for what purposes.

42 Electronic communications marketing

Describe any rules on marketing by e-mail, fax or telephone.

The privacy data law described applies to electronic communications marketing involving the use of personal data. In addition, the Unsolicited Electronic Message Ordinance also regulates spam in prohibiting the use of unscrupulous techniques such as address harvesting software, dictionary or brute force attack to send spam, and fraud or other illicit activities like using hacked or zombie computers to send multiple spam messages. Electronic communications marketing must comply with specified requirements including clear identification of the sender with contact facilities made valid for 30 days minimum, offering opt-out, compliance with opt-out response in 10 working days and no sending to entries on the official do-not-call registers.

Chloe Lee **chloe@jsg.hk**

2410 Dah Sing Financial Centre
108 Gloucester Road
Wanchai
Hong Kong

Tel: +852 3905 1078
Fax: +852 3482 2081
www.jsg.hk