

Data Privacy Laws & Regulations

Hong Kong

Summary Overview

Current Active Law & Regulation:

“PERSONAL DATA (PRIVACY) ORDINANCE” - Enacted in 1995.

The Act is overseen by the Office of the Privacy Commissioner for Personal Data, Hong Kong

Summary Overview:

In this Act, "personal data" means personal information constituting a personal information database, etc. The operative Chapter and Articles are as follows:

Chapter 4. Duties of Business Entities Handling Personal Information

- Restriction by Purpose of Utilization (Article 16)
- Proper Acquisition (Article 17)
- Security Control Measures (Article 20)
- Restriction of Provision to A Third Party (Article 23)
- Disclosure, Correction and Discontinuance of
- Utilization (Articles 25 through 27)

This Act operates as a guideline. A businesses use of personal information must be authorized by the consumer in advance of the information use. For businesses not relying on personal information of their employees for the business operation any disclosure of personal employee information to a third party must be approved by the employee (unless directly subpoenaed by a legal action) – Article 23 Paragraph 1. of the Act.

Weblink to Hong Kong Government Act Source Site:

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

Attachments to Summary:

- 1) Personal Data Privacy Ordinance

Summary Author: This summary overview is contributed to the Sedona Conference by Mr. Andrew Dale, Partner and Hong Kong Office Partner for Orrick, Herrington & Sutcliffe LLP.

Prepared Exclusively for The Sedona Conference – May, 2011. This Summary is not a legal opinion, cannot be relied upon for legal positions and is provided as an informational source only.

Chapter:	486	PERSONAL DATA (PRIVACY) ORDINANCE	Gazette Number	Version Date
----------	-----	-----------------------------------	----------------	--------------

		Long title		30/06/1997
--	--	------------	--	------------

An Ordinance to protect the privacy of individuals in relation to personal data, and to provide for matters incidental thereto or connected therewith.

(Enacted 1995)

[Part II, section 71 (as affects Schedule 2) and Schedule 2	}	1 August 1996	<i>L.N. 343 of 1996</i>
The other provisions, excluding sections 30 and 33	}	20 December 1996	<i>L.N. 514 of 1996</i>
Section 30	}	1 August 1997	<i>L.N. 409 of 1997]</i>

(Originally 81 of 1995)

Section:	1	Short title and commencement	L.N. 130 of 2007	01/07/2007
----------	---	------------------------------	------------------	------------

Remarks:

For the saving and transitional provisions relating to the amendments made by the Resolution of the Legislative Council (L.N. 130 of 2007), see paragraph (12) of that Resolution.

PART I

PRELIMINARY

- (1) This Ordinance may be cited as the Personal Data (Privacy) Ordinance.
- (2) This Ordinance shall come into operation on a day to be appointed by the Secretary for Constitutional and Mainland Affairs by notice in the Gazette. (Amended L.N. 130 of 2007)

(Enacted 1995)

Section:	2	Interpretation	L.N. 204 of 2006	01/12/2006
----------	---	----------------	------------------	------------

- (1) In this Ordinance, unless the context otherwise requires-
- "act" (作為) includes a deliberate omission;
- "adverse action" (不利行動), in relation to an individual, means any action that may adversely affect the individual's rights, benefits, privileges, obligations or interests (including legitimate expectations);
- "appointed day" (指定日) means the day appointed under section 1(2);
- "approved code of practice" (核准實務守則) means a code of practice approved under section 12;
- "code of practice" (實務守則) includes-
- (a) a standard;
 - (b) a specification; and
 - (c) any other documentary form of practical guidance;
- "Commissioner" (專員) means the Privacy Commissioner for Personal Data established under section 5(1);
- "Committee" (諮詢委員會) means the Personal Data (Privacy) Advisory Committee established under section 11(1);
- "complainant" (投訴人) means the individual, or the relevant person on behalf of an individual, who has made a complaint;
- "complaint" (投訴) means a complaint under section 37;
- "correction" (改正), in relation to personal data, means rectification, erasure or completion;

"daily penalty" (每日罰款) means a penalty for each day on which the offence is continued after conviction therefor;

"data" (資料) means any representation of information (including an expression of opinion) in any document, and includes a personal identifier;

"data access request" (查閱資料要求) means a request under section 18;

"data correction request" (改正資料要求) means a request under section 22(1);

"data protection principle" (保障資料原則) means any of the data protection principles set out in Schedule 1;

"data subject" (資料當事人), in relation to personal data, means the individual who is the subject of the data;

"data user" (資料使用者), in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data;

"data user return" (資料使用者申報表) means a data user return referred to in section 14(4);

"disclosing" (披露), in relation to personal data, includes disclosing information inferred from the data;

"document" (文件) includes, in addition to a document in writing-

- (a) a disc, tape or other device in which data other than visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the disc, tape or other device; and
- (b) a film, tape or other device in which visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced from the film, tape or other device;

"employment" (僱用) means employment under-

- (a) a contract of service or of apprenticeship; or
- (b) a contract personally to execute any work or labour,

and related expressions shall be construed accordingly;

"enforcement notice" (執行通知) means a notice under section 50(1);

"financial regulator" (財經規管者) means any of-

- (a) the Monetary Authority appointed under section 5A of the Exchange Fund Ordinance (Cap 66);
- (b) the Securities and Futures Commission referred to in section 3(1) of the Securities and Futures Ordinance (Cap 571); (Replaced 5 of 2002 s. 407)
- (c) a recognized clearing house, a recognized exchange company, a recognized exchange controller or a recognized investor compensation company within the meaning of section 1 of Part 1 of Schedule 1 to the Securities and Futures Ordinance (Cap 571); (Replaced 5 of 2002 s. 407)
- (d) a person authorized under Part III of the Securities and Futures Ordinance (Cap 571) to provide automated trading services as defined in Schedule 5 to that Ordinance; (Replaced 5 of 2002 s. 407)
- (e)-(ea) (Repealed 5 of 2002 s. 407)
- (f) the Insurance Authority appointed under section 4 of the Insurance Companies Ordinance (Cap 41);
- (g) the Registrar of Occupational Retirement Schemes appointed under section 5 of the Occupational Retirement Schemes Ordinance (Cap 426);
- (ga) the Mandatory Provident Fund Schemes Authority established by section 6 of the Mandatory Provident Fund Schemes Ordinance (Cap 485); (Added 4 of 1998 s. 14)
- (gb) the Financial Reporting Council established by section 6(1) of the Financial Reporting Council Ordinance (Cap 588); (Added 18 of 2006 s. 84)
- (h) a person specified in a notice under subsection (7) to be a regulator for the purposes of this definition;

"inaccurate" (不準確), in relation to personal data, means the data is incorrect, misleading, incomplete or obsolete;

"inspection" (視察) means an inspection under section 36;

"investigation" (調查) means an investigation under section 38;

"log book" (紀錄簿), in relation to a data user, means the log book kept and maintained by the data user under section 27(1);

"matching procedure" (核對程序) means any procedure whereby personal data collected for 1 or more purposes in respect of 10 or more data subjects are compared (except by manual means) with personal data collected for any other purpose in respect of those data subjects where the comparison-

- (a) is (whether in whole or in part) for the purpose of producing or verifying data that; or
- (b) produces or verifies data in respect of which it is reasonable to believe that it is practicable that the data,

may be used (whether immediately or at any subsequent time) for the purpose of taking adverse action against any of those data subjects;

"matching procedure request" (核對程序要求) means a request under section 31(1);

"personal data" (個人資料) means any data-

- (a) relating directly or indirectly to a living individual;
- (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and
- (c) in a form in which access to or processing of the data is practicable;

"personal data system" (個人資料系統) means any system, whether or not automated, which is used, whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system;

"personal identifier" (個人身分標識符) means an identifier-

- (a) that is assigned to an individual by a data user for the purpose of the operations of the user; and
- (b) that uniquely identifies that individual in relation to the data user,

but does not include an individual's name used to identify that individual;

"practicable" (切實可行) means reasonably practicable;

"prescribed officer" (訂明人員) means a person employed or engaged under section 9(1);

"processing" (處理), in relation to personal data, includes amending, augmenting, deleting or rearranging the data, whether by automated means or otherwise;

"register" (登記冊) means the register of data users kept and maintained by the Commissioner under section 15(1);

"relevant data user" (有關資料使用者), in relation to-

- (a) an inspection, means the data user who uses the personal data system which is the subject of the inspection;
- (b) a complaint, means the data user specified in the complaint;
- (c) an investigation-
 - (i) in the case of an investigation initiated by a complaint, means the data user specified in the complaint;
 - (ii) in any other case, means the data user the subject of the investigation;
- (d) an enforcement notice, means the data user on whom the notice is served;

"relevant person" (有關人士), in relation to an individual (howsoever the individual is described), means-

- (a) where the individual is a minor, a person who has parental responsibility for the minor;
- (b) where the individual is incapable of managing his own affairs, a person who has been appointed by a court to manage those affairs;
- (c) in any other case, a person authorized in writing by the individual to make a data access request, a data correction request, or both such requests, on behalf of the individual;

"requestor" (提出要求者), in relation to-

- (a) a data access request or data correction request, means the individual, or the relevant person on behalf of an individual, who has made the request;
- (b) a matching procedure request, means the data user who has made the request;

"specified" (指明), in relation to a form, means specified under section 67;

"third party" (第三者), in relation to personal data, means any person other than-

- (a) the data subject;
- (b) a relevant person in the case of the data subject;
- (c) the data user; or
- (d) a person authorized in writing by the data user to collect, hold, process or use the data-
 - (i) under the direct control of the data user; or
 - (ii) on behalf of the data user;

"use" (使用), in relation to personal data, includes disclose or transfer the data;

"would be likely to prejudice" (相當可能損害) includes would prejudice.

(2) For the avoidance of doubt, it is hereby declared that paragraph (c) of the definition of "relevant person" shall not be construed-

- (a) to entitle a person who has only been authorized to make a data access request on behalf of an individual to make a data correction request on behalf of the individual;
 - (b) to entitle a person who has only been authorized to make a data correction request on behalf of an individual to make a data access request on behalf of the individual.
- (3) Where under this Ordinance an act may be done with the prescribed consent of a person (and howsoever the person is described), such consent-
- (a) means the express consent of the person given voluntarily;
 - (b) does not include any consent which has been withdrawn by notice in writing served on the person to whom the consent has been given (but without prejudice to so much of that act that has been done pursuant to the consent at any time before the notice is so served).
- (4) Subject to section 64(10), it is hereby declared that any reference in this Ordinance to the effect that a data user (howsoever described)-
- (a) has contravened a requirement under this Ordinance; or
 - (b) is contravening a requirement under this Ordinance,
- includes-
- (i) where paragraph (a) is applicable, any case where the data user has done an act, or engaged in a practice, in contravention of a data protection principle;
 - (ii) where paragraph (b) is applicable, any case where the data user is doing an act, or engaging in a practice, in contravention of a data protection principle.
- (5) Notwithstanding any other provisions of this Ordinance, a complaint may be made (and an investigation, if any, initiated by the complaint may be carried out) in relation to a person who has ceased to be a data user except any such person who has not at any time been a data user during the period of 2 years immediately preceding the date on which the Commissioner receives the complaint and, accordingly, a person in relation to whom such a complaint is made shall for the purposes of such complaint (and an investigation, if any, initiated by such complaint) be deemed to be a data user, and the other provisions of this Ordinance shall be construed accordingly.
- (6) Any reference in this Ordinance to a data protection principle followed by a number is a reference to the principle bearing that number set out in Schedule 1.
- (7) The Chief Executive may, by notice in the Gazette, specify a person to be a regulator for the purposes of the definition of "financial regulator". (Amended 34 of 1999 s. 3)
- (8) It is hereby declared that a notice under subsection (7) is subsidiary legislation.
- (9) Where a person-
- (a) holds any office, engages in any profession or carries on any occupation; and
 - (b) is required by any law, or by any rules made under or by virtue of any law, to be a fit and proper person (or words to the like effect) to hold that office, engage in that profession or carry on that occupation,
- then, for the purposes of this Ordinance, any conduct by that person by virtue of which he ceases, or would cease, to be such a fit and proper person shall be deemed to be seriously improper conduct.
- (10) Subsection (9) shall not operate to prevent seriously improper conduct including, for the purposes of this Ordinance, conduct by virtue of which a person ceases, or would cease, to be a fit and proper person notwithstanding that the conduct is not conduct to which that subsection applies.
- (11) Words and expressions importing the neuter gender in relation to any data user shall include the masculine and feminine genders.
- (12) A person is not a data user in relation to any personal data which the person holds, processes or uses solely on behalf of another person if, but only if, that first-mentioned person does not hold, process or use, as the case may be, those data for any of his own purposes.
- (13) For the avoidance of doubt, it is hereby declared that, for the purposes of this Ordinance, any conduct by a person by virtue of which he has or could become a disqualified person or a suspended person under the Rules of Racing and Instructions by the Stewards of the Hong Kong Jockey Club, as in force from time to time, is seriously improper conduct. (Amended 34 of 1999 s. 3)

(Enacted 1995)

Section:	3	Application		01/07/1997
----------	---	-------------	--	------------

- (1) This Ordinance binds the Government.
- (2) (*Not adopted as the laws of HKSAR)

(Enacted 1995)

Note:

* See Decision of the Standing Committee of the National People's Congress on Treatment of the Laws Previously in Force in Hong Kong in accordance with Article 160 of the Basic Law of the Hong Kong Special Administrative Region of the People's Republic of China, which is published in Volume 1, p. 13/1.

Section:	4	Data protection principles		30/06/1997
----------	---	----------------------------	--	------------

A data user shall not do an act, or engage in a practice, that contravenes a data protection principle unless the act or practice, as the case may be, is required or permitted under this Ordinance.

(Enacted 1995)

Section:	5	Establishment, etc. of Privacy Commissioner for Personal Data	34 of 1999	01/07/1997
----------	---	---	------------	------------

Remarks:

Adaptation amendments retroactively made - see 34 of 1999 s. 3

PART II

ADMINISTRATION

(1) For the purposes of this Ordinance, there is hereby established an office by the name of the Privacy Commissioner for Personal Data.

(2) The Commissioner shall be a corporation sole with perpetual succession and-

- (a) shall have and may use a seal; and
- (b) shall be capable of suing and being sued.

(3) The Chief Executive shall, by notice in the Gazette, appoint a person to be the Commissioner. (Amended 34 of 1999 s. 3)

(4) Subject to subsection (5), the person appointed to be the Commissioner shall hold office for a period of 5 years and shall be eligible for reappointment for not more than 1 further period of 5 years.

(5) The person appointed to be the Commissioner may-

- (a) at any time resign from his office by notice in writing to the Chief Executive; or
- (b) be removed from office by the Chief Executive with the approval by resolution of the Legislative Council on the ground of-
 - (i) inability to perform the functions of his office; or
 - (ii) misbehaviour. (Amended 34 of 1999 s. 3)

(6) The Chief Executive shall determine- (Amended 34 of 1999 s. 3)

- (a) the emoluments; and
- (b) the terms and conditions of appointment,

of the person appointed to be the Commissioner.

(7) The provisions of Schedule 2 shall have effect with respect to the Commissioner.

(8) Subject to subsection (9), the Commissioner shall not be regarded as a servant or agent of the Government or as enjoying any status, immunity or privilege of the Government.

(9) The person appointed to be the Commissioner shall be deemed to be a public servant-

- (a) within the meaning of section 2 of the Prevention of Bribery Ordinance (Cap 201); and
- (b) for the purposes of that Ordinance.

(Enacted 1995)

Section:	6	Commissioner to hold no other office	34 of 1999	01/07/1997
----------	---	--------------------------------------	------------	------------

Remarks:

Adaptation amendments retroactively made - see 34 of 1999 s. 3

The person appointed to be the Commissioner shall not, without the specific approval of the Chief Executive- (Amended 34 of 1999 s. 3)

- (a) hold any office of profit other than his office as Commissioner; or
- (b) engage in any occupation for reward outside the functions of his office.

(Enacted 1995)

Section:	7	Filling of temporary vacancy	34 of 1999	01/07/1997
----------	---	------------------------------	------------	------------

Remarks:

Adaptation amendments retroactively made - see 34 of 1999 s. 3

- (1) Where the person appointed to be the Commissioner-
 - (a) dies;
 - (b) resigns;
 - (c) is removed from office;
 - (d) is absent from Hong Kong; or
 - (e) is for any other reason unable to perform the functions of his office,then the Chief Executive may, by notice in writing, appoint a person to act as the Commissioner until, as the case requires- (Amended 34 of 1999 s. 3)
 - (i) a new Commissioner is appointed under section 5(3); or
 - (ii) the Commissioner resumes his office.
- (2) A person appointed under subsection (1) to act as the Commissioner, whilst he is so appointed-
 - (a) shall perform the functions; and
 - (b) may exercise the powers,of the Commissioner under this Ordinance.
- (3) Section 6 shall apply to a person appointed under subsection (1) to act as the Commissioner as if that person were the Commissioner.

(Enacted 1995)

Section:	8	Functions and powers of Commissioner	34 of 1999	01/07/1997
----------	---	--------------------------------------	------------	------------

Remarks:

Adaptation amendments retroactively made - see 34 of 1999 s. 3

- (1) The Commissioner shall-
 - (a) monitor and supervise compliance with the provisions of this Ordinance;
 - (b) promote and assist bodies representing data users to prepare, for the purposes of section 12, codes of practice for guidance in complying with the provisions of this Ordinance, in particular the data protection principles;
 - (c) promote awareness and understanding of, and compliance with, the provisions of this Ordinance, in particular the data protection principles;
 - (d) examine 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 person proposing the legislation;
 - (e) carry out inspections, including inspections of any personal data systems used by data users which are departments of the Government or statutory corporations;
 - (f) for the better performance of his other functions, undertake research into, and monitor developments in, the processing of data and computer technology in order to take account of any likely adverse effects such developments may have on the privacy of individuals in relation to personal data;
 - (g) liaise and co-operate with any person in any place outside Hong Kong-
 - (i) performing in that place any functions which, in the opinion of the Commissioner, are similar (whether in whole or in part) to any of the Commissioner's functions under this Ordinance; and
 - (ii) in respect of matters of mutual interest concerning the privacy of individuals in relation to personal data; and
 - (h) perform such other functions as are imposed on him under this Ordinance or any other enactment.

(2) The Commissioner may do all such things as are necessary for, or incidental or conducive to, the better performance of his functions and in particular but without prejudice to the generality of the foregoing, may-

- (a) acquire and hold property of any description if in the opinion of the Commissioner such property is necessary for-
 - (i) the accommodation of the Commissioner or of any prescribed officer; or
 - (ii) the performance of any function which the Commissioner may perform, and, subject to the terms and conditions upon which such property is held, dispose of it;
- (b) enter into, carry out, assign or accept the assignment of, vary or rescind, any contract, agreement or other obligation;
- (c) undertake and execute any lawful trust which has as an object the furtherance of any function which the Commissioner is required or is permitted by this Ordinance to perform or any other similar object;
- (d) accept gifts and donations, whether subject to any trust or not;
- (e) with the prior approval of the Chief Executive, become a member of or affiliate to any international body concerned with (whether in whole or in part) the privacy of individuals in relation to personal data; (Amended 34 of 1999 s. 3)
- (f) exercise such other powers as are conferred on him under this Ordinance or any other enactment.

(3) The Commissioner may make and execute any document in the performance of his functions or the exercise of his powers or in connection with any matter reasonably incidental to or consequential upon the performance of his functions or the exercise of his powers.

(4) Any document purporting to be executed under the seal of the Commissioner shall be admitted in evidence and shall, in the absence of evidence to the contrary, be deemed to have been duly executed.

(5) The Commissioner may from time to time cause to be prepared and published by notice in the Gazette, for the guidance of data users, guidelines not inconsistent with this Ordinance, indicating the manner in which he proposes to perform any of his functions, or exercise any of his powers, under this Ordinance.

(Enacted 1995)

Section:	9	Staff of Commissioner, etc.	30/06/1997
----------	---	-----------------------------	------------

- (1) The Commissioner may-
 - (a) employ such persons (including technical and professional persons); and
 - (b) engage, other than by way of employment, such technical and professional persons,as he thinks fit to assist him in the performance of his functions, and the exercise of his powers, under this Ordinance.
- (2) The Commissioner shall determine-
 - (a) the remuneration and terms and conditions of employment of any person, or any person belonging to a class of persons, who may be employed under subsection (1)(a);
 - (b) the remuneration and terms and conditions of engagement of any person, or any person belonging to a class of persons, who may be engaged under subsection (1)(b).
- (3) The Commissioner may-
 - (a) grant, or make provision for the grant of, pensions, gratuities and retirement benefits to employees;
 - (b) provide other benefits for the welfare of employees and their dependants;
 - (c) authorize payments, whether or not legally due, to the personal representatives of a deceased employee or to any person who was dependent on such employee at his death.
- (4) The Commissioner may-
 - (a) establish, manage and control; or
 - (b) enter into an arrangement with any company or association for the establishment, management and control by that company or association either alone or jointly with the Commissioner of,any fund or scheme for the purpose of providing for the pensions, gratuities, benefits and payments referred to in subsection (3).
- (5) The Commissioner may make contributions to and may require employees to make contributions to any fund or scheme referred to in subsection (4).
- (6) In this section "employees" (僱員) includes any class of employee which the Commissioner specifies and in subsection (3) includes former employees.

(Enacted 1995)

Section:	10	Delegations by Commissioner		30/06/1997
----------	----	-----------------------------	--	------------

(1) Subject to subsection (2), the Commissioner may delegate in writing any of his functions or powers under this Ordinance to any prescribed officer subject to such terms and conditions, if any, as he thinks fit and specified in the delegation.

(2) The Commissioner shall not delegate any of his functions or powers under-

- (a) subsection (1);
- (b) any provisions of any regulations made under this Ordinance which are specified in the regulations as provisions which shall not be subject to subsection (1);
- (c) any provisions of Schedule 2 which are specified in that Schedule as provisions which shall not be subject to subsection (1).

(3) A delegate of the Commissioner-

- (a) shall perform the delegated functions and may exercise the delegated powers as if the delegate were the Commissioner; and
- (b) shall be presumed to be acting in accordance with the relevant delegation in the absence of evidence to the contrary.

(Enacted 1995)

Section:	11	Establishment of Personal Data (Privacy) Advisory Committee	L.N. 130 of 2007	01/07/2007
----------	----	---	------------------	------------

Remarks:

For the saving and transitional provisions relating to the amendments made by the Resolution of the Legislative Council (L.N. 130 of 2007), see paragraph (12) of that Resolution.

(1) There is hereby established a committee by the name of the Personal Data (Privacy) Advisory Committee for the purpose of advising the Commissioner upon any matter relevant to the privacy of individuals in relation to personal data or otherwise relevant to the operation of this Ordinance.

(2) The Committee shall consist of-

- (a) the Commissioner, who shall be the chairman; and
- (b) not less than 4 or more than 8 other persons, appointed by the Secretary for Constitutional and Mainland Affairs, of whom-
 - (i) not less than 1 shall have not less than 5 years' experience in the processing of data; and
 - (ii) not more than 1 shall be a public officer.

(3) The members of the Committee appointed under subsection (2)(b) shall hold office for such period and upon such terms as the Secretary for Constitutional and Mainland Affairs specifies in their respective appointments or from time to time.

(4) A member of the Committee appointed under subsection (2)(b) may resign at any time by notice in writing delivered to the Secretary for Constitutional and Mainland Affairs.

(5) The Committee may regulate its procedure.

(Enacted 1995. Amended L.N. 130 of 2007)

Section:	12	Approval of codes of practice by Commissioner		30/06/1997
----------	----	---	--	------------

PART III

CODES OF PRACTICE

(1) Subject to subsections (8) and (9), for the purpose of providing practical guidance in respect of any requirements under this Ordinance imposed on data users, the Commissioner may-

- (a) approve and issue such codes of practice (whether prepared by him or not) as in his opinion are suitable for that purpose; and
- (b) approve such codes of practice issued or proposed to be issued otherwise than by him as in his opinion are suitable for that purpose.

(2) Where a code of practice is approved under subsection (1), the Commissioner shall, by notice in the Gazette-

- (a) identify the code concerned and specify the date on which its approval is to take effect; and
 - (b) specify for which of the requirements under this Ordinance the code is so approved.
- (3) The Commissioner may-
- (a) from time to time revise the whole or any part of any code of practice prepared by him under this section; and
 - (b) approve any revision or proposed revision of the whole or any part of any code of practice for the time being approved under this section,

and the provisions of subsection (2) shall, with the necessary modifications, apply in relation to the approval of any revision under this subsection as they apply in relation to the approval of a code of practice under subsection (1).

(4) The Commissioner may at any time withdraw his approval from any code of practice approved under this section.

(5) Where under subsection (4) the Commissioner withdraws his approval from a code of practice approved under this section, he shall, by notice in the Gazette, identify the code concerned and specify the date on which his approval of it is to cease to have effect.

(6) References in this Ordinance to an approved code of practice are references to that code as it has effect for the time being by virtue of any revision of the whole or any part of it approved under this section.

(7) The power of the Commissioner under subsection (1)(b) to approve a code of practice issued or proposed to be issued otherwise than by him shall include power to approve a part of such a code and, accordingly, in this Ordinance "code of practice" (實務守則) may be read as including a part of such a code.

(8) The Commissioner shall, not later than 6 months after the day on which this section comes into operation (or within such further period, not exceeding 6 months, as the Secretary for Home Affairs may allow), approve a code of practice under subsection (1) in respect of all or any requirements referred to in that subsection in so far as such requirements relate to personal data which are personal identifiers.

(9) The Commissioner shall, before approving a code of practice under subsection (1) or any revision or proposed revision of the code under subsection (3), consult with-

- (a) such bodies representative of data users to which the code or the code as so revised, as the case may be, will apply (whether in whole or in part); and
- (b) such other interested persons,

as he thinks fit.

(10) For the avoidance of doubt, it is hereby declared that different codes of practice may be approved under subsection (1) (including any code of practice referred to in subsection (8)) for different classes of data users, and may be so approved for the same or different requirements referred to in subsection (1).

(Enacted 1995)

Section:	13	Use of approved codes of practice in proceedings under this Ordinance		30/06/1997
----------	----	---	--	------------

(1) A failure on the part of any data user to observe any provision of an approved code of practice shall not of itself render the data user liable to any civil or criminal proceedings but where in any proceedings under this Ordinance a data user is alleged to have contravened a requirement under this Ordinance, being a requirement for which there was an approved code of practice at the time of the alleged contravention, subsection (2) shall have effect with respect to such code in relation to those proceedings.

(2) Any provision of a code of practice which appears to a specified body to be relevant to a requirement under this Ordinance alleged to have been contravened shall be admissible in evidence in the proceedings under this Ordinance concerned and if it is proved that there was at any material time a failure to observe any provision of the code which appears to that body to be relevant to any matter which it is necessary to prove in order to establish a contravention of such requirement, that matter shall be taken as proved in the absence of evidence that such requirement was in respect of that matter complied with otherwise than by way of observance of that provision.

(3) In any proceedings under this Ordinance, a code of practice which appears to a specified body to be the subject of a notice under section 12 shall be taken to be the subject of such notice in the absence of evidence to the contrary.

(4) In this section-

"proceedings under this Ordinance" (根據本條例進行的法律程序) includes any criminal proceedings where a data user is alleged to have committed an offence by reason of a contravention of a requirement under this Ordinance;

"specified body" (指明當局) means-

- (a) a magistrate;
- (b) a court; or
- (c) the Administrative Appeals Board.

(Enacted 1995)

Section:	14	Data user returns	L.N. 130 of 2007	01/07/2007
----------	----	-------------------	------------------	------------

Remarks:

For the saving and transitional provisions relating to the amendments made by the Resolution of the Legislative Council (L.N. 130 of 2007), see paragraph (12) of that Resolution.

PART IV

DATA USER RETURNS AND REGISTER OF DATA USERS

(1) Subject to subsection (2), the Commissioner may, by notice in the Gazette, specify a class of data users to which this section shall apply.

(2) The Commissioner shall, before specifying a class of data users in a notice under subsection (1), consult with-

- (a) such bodies representative of data users belonging to that class; and
- (b) such other interested persons,

as he thinks fit.

(3) This section shall not apply to a data user except a data user belonging to a class of data users specified in a notice under subsection (1) which is in force.

(4) A data user shall submit to the Commissioner a data user return-

- (a) in the specified form;
- (b) containing the prescribed information required by the return in relation to the data user;
- (c) in the case of-
 - (i) a data user which belongs to the class of data users concerned on the day on which the notice under subsection (1) specifying that class commences, not earlier than 3 months before, and not later than, each anniversary of that day;
 - (ii) a data user which first belongs to the class of data users concerned on a day after the day on which the notice under subsection (1) specifying that class commences, not earlier than 3 months before, and not later than, each anniversary of that first-mentioned day; and

(d) accompanied by the prescribed fee.

(5) The Commissioner shall cause a notice to be published not less than once during every period of 6 months-

- (a) in-
 - (i) the Gazette; and
 - (ii) not less than 1 Chinese language newspaper (and in the Chinese language) and not less than 1 English language newspaper (and in the English language), each of which shall be a newspaper circulating generally in Hong Kong; and
- (b) subject to subsection (6), specifying the places at which and the hours during which data user returns are available to be obtained by data users for the purposes of this section.

(6) The Commissioner shall not exercise his power under subsection (5)(b) to specify places which are Government offices unless and until he has the approval in writing of the Secretary for Constitutional and Mainland Affairs to do so. (Amended L.N. 130 of 2007)

(7) The Commissioner shall cause data user returns to be available to be obtained by data users-

- (a) free of charge; and
- (b) at the places and during the hours specified in the last notice published under subsection (5).

(8) Where any prescribed information contained in a data user return submitted under subsection (4) to the Commissioner by a data user changes subsequent to the submission, then the data user shall serve a notice in writing on the Commissioner specifying such change-

- (a) if, but only if-
 - (i) such information is specified in the return as information to which this subsection applies; and

- (ii) the return contains, or has annexed to it-
 - (A) a copy of this subsection; or
 - (B) a statement summarizing the requirement imposed by this subsection on the data user; and
 - (b) not later than 30 days after such change.
- (9) It is hereby declared that-
 - (a) a notice under subsection (1) is subsidiary legislation;
 - (b) where a data user belongs to 2 or more classes of data users specified in 2 or more notices under subsection (1) which are in force, then, for the purposes of this section, that data user shall be deemed to belong only to that class of data users specified in the first of those notices to be published in the Gazette; and
 - (c) subsection (3) shall not operate to prejudice the generality of section 67(4)(c).
- (10) In this section and section 15, "prescribed information" (訂明資訊) means any information specified in Schedule 3.

(Enacted 1995)

Section:	15	Register of data users		30/06/1997
----------	----	------------------------	--	------------

- (1) The Commissioner shall use-
 - (a) data user returns submitted to him under section 14(4); and
 - (b) any notices served on him under section 14(8),
 to keep and maintain a register of data users which have submitted such returns.
- (2) The register shall-
 - (a) be in the form of a database; and
 - (b) contain, in respect of each data user who has submitted a data user return under section 14(4), such particulars of the information supplied in that return as the Commissioner thinks fit.
- (3) The Commissioner may, by notice in writing served on a data user, require the data user to submit a notice in the prescribed form containing such prescribed information in relation to the data user as the Commissioner may reasonably require in order to keep and maintain the register in so far as it relates to that data user, and the data user shall so submit the second-mentioned notice within such period (being a period of not less than 30 days after service of the first-mentioned notice) and in such manner as the Commissioner requires in the first-mentioned notice.
- (4) Where any prescribed information submitted to the Commissioner under subsection (3) by a data user changes subsequent to the submission, then the data user shall serve a notice in writing on the Commissioner specifying such change-
 - (a) if, but only if-
 - (i) such information is specified in the notice concerned under that subsection as information to which this subsection applies; and
 - (ii) the notice referred to in subparagraph (i) contains, or has annexed to it-
 - (A) a copy of this subsection; or
 - (B) a statement summarizing the requirement imposed by this subsection on the data user; and
 - (b) not later than 30 days after such change.
- (5) If the Commissioner is satisfied that a person has ceased to be a data user, he may delete from the register any particulars contained therein relating to that person in that person's capacity as a data user.
- (6) A person who has ceased to be a data user may, by notice in the specified form served on the Commissioner, request the Commissioner to delete from the register the particulars contained therein relating to that person in that person's capacity as a data user, and the Commissioner shall, not later than 3 months after the date on which he receives that notice, comply with that request unless it has been withdrawn by that person.

(Enacted 1995)

Section:	16	Inspection of register		30/06/1997
----------	----	------------------------	--	------------

- (1) The Commissioner shall provide facilities for making the particulars contained in the register available for inspection-
 - (a) by any person;
 - (b) in visible and legible form;

- (c) during ordinary office hours; and
- (d) free of charge.
- (2) The Commissioner shall-
 - (a) on receipt of an application in the specified form from a person; and
 - (b) on payment of the prescribed fee,

provide a copy in writing of the particulars contained in the register in respect of the data user, or the class of data users, specified in the application.

(Enacted 1995)

Section:	17	Register shall not limit, etc. operation of this Ordinance		30/06/1997
----------	----	--	--	------------

- (1) For the avoidance of doubt, it is hereby declared that-
 - (a) whether or not the register contains any particulars;
 - (b) any particulars contained in the register,
 in respect of a data user shall not of itself-
 - (i) limit, restrict or qualify the operation of any of the provisions of this Ordinance (including section 2(5) and the data protection principles) in relation to the data user;
 - (ii) exempt the data user from the operation of any of the provisions of this Ordinance.
- (2) Subsection (1) shall not prejudice the operation of any limitation, restriction, qualification or exemption provided for in the other provisions of this Ordinance.

(Enacted 1995)

Section:	18	Data access request		30/06/1997
----------	----	---------------------	--	------------

PART V

ACCESS TO AND CORRECTION OF PERSONAL DATA

- (1) An individual, or a relevant person on behalf of an individual, may make a request-
 - (a) to be informed by a data user whether the data user holds personal data of which the individual is the data subject;
 - (b) if the data user holds such data, to be supplied by the data user with a copy of such data.
- (2) A data access request under both paragraphs of subsection (1) shall be treated as being a single request, and the provisions of this Ordinance shall be construed accordingly.
- (3) A data access request under paragraph (a) of subsection (1) may, in the absence of evidence to the contrary, be treated as being a data access request under both paragraphs of that subsection, and the provisions of this Ordinance (including subsection (2)) shall be construed accordingly.
- (4) A data user who, in relation to personal data-
 - (a) does not hold the data; but
 - (b) controls the use of the data in such a way as to prohibit the data user who does hold the data from complying (whether in whole or in part) with a data access request which relates to the data,
 shall be deemed to hold those data, and the provisions of this Ordinance (including this section) shall be construed accordingly.

(Enacted 1995)

Section:	19	Compliance with data access request		30/06/1997
----------	----	-------------------------------------	--	------------

- (1) Subject to subsection (2) and sections 20 and 28(5), a data user shall comply with a data access request not later than 40 days after receiving the request.
- (2) A data user who is unable to comply with a data access request within the period specified in subsection (1) shall-
 - (a) before the expiration of that period-
 - (i) by notice in writing inform the requestor that the data user is so unable and of the reasons why the data user is so unable; and
 - (ii) comply with the request to the extent, if any, that the data user is able to comply with the request;

and

(b) as soon as practicable after the expiration of that period, comply or fully comply, as the case may be, with the request.

(3) A copy of the personal data to be supplied by a data user in compliance with a data access request shall-

(a) be supplied by reference to the data at the time when the request is received except that the copy may take account of-

(i) any processing of the data-

(A) made between that time and the time when the copy is supplied; and

(B) that would have been made irrespective of the receipt of the request; and

(ii) subject to subsection (5), any correction to the data made between that time and the time when the copy is supplied;

(b) where any correction referred to paragraph (a)(ii) has been made to the data, be accompanied by a notice stating that the data have been corrected pursuant to that paragraph (or words to the like effect); and

(c) as far as practicable, be-

(i) intelligible unless the copy is a true copy of a document which-

(A) contains the data; and

(B) is unintelligible on its face;

(ii) readily comprehensible with any codes used by the data user adequately explained; and

(iii) in-

(A) subject to sub-subparagraph (B), the language specified in the request or, if no language is so specified, the language in which the request is made (which may be the Chinese or English language in either case);

(B) a language other than the language specified in the request or, if no language is so specified, the language in which the request is made, if, but only if-

(I) the language in which the data are held is not the language specified in the request or, if no language is so specified, the language in which the request is made, as the case may be; and

(II) subject to section 20(2)(b), the copy is a true copy of a document which contains the data;

(iv) without prejudice to the generality of subparagraph (iii) but subject to subsection (4), be in the form, or one of the forms, if any, specified in the request;

(v) where subparagraph (iv) is not applicable, in such form as the data user thinks fit.

(4) Where-

(a) a data access request specifies the form or forms in which a copy of the personal data to be supplied in compliance with the request is or are sought; and

(b) the data user concerned is unable to supply the copy in that form or any of those forms, as the case may be, because it is not practicable for the data user to do so,

then the data user shall-

(i) where there is only one form in which it is practicable for the data user to supply the copy, supply the copy in that form accompanied by a notice in writing informing the requestor that that form is the only form in which it is practicable for the data user to supply the copy;

(ii) in any other case-

(A) as soon as practicable, by notice in writing inform the requestor-

(I) that it is not practicable for the data user to supply the copy in the form or any of the forms, as the case may be, specified in the request;

(II) of the forms in which it is practicable for the data user to supply the copy; and

(III) that the requestor may, not later than 14 days after the requestor has received the notice, specify in writing one of the forms referred to in sub-subparagraph (II) in which the copy is to be supplied; and

(B) as soon as practicable, supply the copy-

(I) in the form specified in the response, if any, to the notice referred to in subparagraph (A);

(II) if there is no such response within the period specified in subparagraph (A)(III), supply the copy in any one of the forms referred to in subparagraph (A)(II) as the data user thinks fit.

(5) Subparagraph (ii) of paragraph (a) and paragraph (b) of subsection (3) shall expire on the 1st anniversary of

the appointed day.

(Enacted 1995)

Section:	20	Circumstances in which data user shall or may refuse to comply with data access request		30/06/1997
----------	----	---	--	------------

- (1) A data user shall refuse to comply with a data access request-
 - (a) if the data user is not supplied with such information as the data user may reasonably require-
 - (i) in order to satisfy the data user as to the identity of the requestor;
 - (ii) where the requestor purports to be a relevant person, in order to satisfy the data user-
 - (A) as to the identity of the individual in relation to whom the requestor purports to be such a person; and
 - (B) that the requestor is such a person in relation to that individual;
 - (b) subject to subsection (2), if the data user cannot comply with the request without disclosing personal data of which any other individual is the data subject unless the data user is satisfied that the other individual has consented to the disclosure of the data to the requestor; or
 - (c) in any other case, if compliance with the request is for the time being prohibited under this Ordinance.
- (2) Subsection (1)(b) shall not operate-
 - (a) so that the reference in that subsection to personal data of which any other individual is the data subject includes a reference to information identifying that individual as the source of the personal data to which the data access request concerned relates unless that information names or otherwise explicitly identifies that individual;
 - (b) so as to excuse a data user from complying with the data access request concerned to the extent that the request may be complied with without disclosing the identity of the other individual, whether by the omission of names, or other identifying particulars, or otherwise.
- (3) A data user may refuse to comply with a data access request if-
 - (a) the request is not in writing in the Chinese or English language;
 - (b) the data user is not supplied with such information as the data user may reasonably require to locate the personal data to which the request relates;
 - (c) the request follows 2 or more similar requests made by-
 - (i) the individual who is the data subject in respect of the personal data to which the request relates;
 - (ii) one or more relevant persons on behalf of that individual; or
 - (iii) any combination of that individual and those relevant persons,and it is unreasonable in all the circumstances for the data user to comply with the request;
 - (d) subject to subsection (4), any other data user controls the use of the data in such a way as to prohibit the first-mentioned data user from complying (whether in whole or in part) with the request;
 - (e) the form in which the request shall be made has been specified under section 67 and the request is not made in that form; or
 - (f) in any other case, compliance with the request may for the time being be refused under this Ordinance, whether by virtue of an exemption under Part VIII or otherwise.
- (4) Subsection (3)(d) shall not operate so as to excuse a data user from complying with the data access request concerned-
 - (a) in so far as the request relates to section 18(1)(a), to any extent;
 - (b) in so far as the request relates to section 18(1)(b), to any extent that the data user can comply with the request without contravening the prohibition concerned.

(Enacted 1995)

Section:	21	Notification of refusal to comply with data access request		30/06/1997
----------	----	--	--	------------

- (1) Subject to subsection (2), a data user who pursuant to section 20 refuses to comply with a data access request shall, as soon as practicable but, in any case, not later than 40 days after receiving the request, by notice in writing inform the requestor-
 - (a) of the refusal;
 - (b) subject to subsection (2), of the reasons for the refusal; and
 - (c) where section 20(3)(d) is applicable, of the name and address of the other data user concerned.

(2) Where-

(a) a data user has pursuant to section 20 refused to comply with a data access request; and

(b) the refusal also relates to section 18(1)(a) by virtue of section 63,

then the data user may, in the notice under subsection (1) concerned, in place of the matters of which the data user is required to inform the requestor under that subsection, inform the requestor that the data user has no personal data the existence of which he is required to disclose to the requestor (or words to the like effect).

(Enacted 1995)

Section:	22	Data correction request		30/06/1997
----------	----	-------------------------	--	------------

(1) Subject to subsection (2), where-

(a) a copy of personal data has been supplied by a data user in compliance with a data access request; and

(b) the individual, or a relevant person on behalf of the individual, who is the data subject considers that the data are inaccurate,

then that individual or relevant person, as the case may be, may make a request that the data user make the necessary correction to the data.

(2) A data user who, in relation to personal data-

(a) does not hold the data; but

(b) controls the processing of the data in such a way as to prohibit the data user who does hold the data from complying (whether in whole or in part) with section 23(1) in relation to a data correction request which relates to the data,

shall be deemed to be a data user to whom such a request may be made, and the provisions of this Ordinance (including subsection (1)) shall be construed accordingly.

(3) Without prejudice to the generality of sections 23(1)(c) and 25(2), if a data user, subsequent to the receipt of a data correction request but before complying with the request pursuant to section 24 or refusing to comply with the request pursuant to section 25, discloses to a third party the personal data to which the request relates, then the user shall take all practicable steps to advise the third party that the data are the subject of a data correction request still under consideration by the user (or words to the like effect).

(Enacted 1995)

Section:	23	Compliance with data correction request		30/06/1997
----------	----	---	--	------------

(1) Subject to subsection (2) and section 24, a data user who is satisfied that personal data to which a data correction request relates are inaccurate shall, not later than 40 days after receiving the request-

(a) make the necessary correction to those data;

(b) supply the requestor with a copy of those data as so corrected; and

(c) subject to subsection (3), if-

(i) those data have been disclosed to a third party during the 12 months immediately preceding the day on which the correction is made; and

(ii) the data user has no reason to believe that the third party has ceased using those data for the purpose (including any directly related purpose) for which the data were disclosed to the third party,

take all practicable steps to supply the third party with a copy of those data as so corrected accompanied by a notice in writing stating the reasons for the correction.

(2) A data user who is unable to comply with subsection (1) in relation to a data correction request within the period specified in that subsection shall-

(a) before the expiration of that period-

(i) by notice in writing inform the requestor that the data user is so unable and of the reasons why the data user is so unable; and

(ii) comply with that subsection to the extent, if any, that the data user is able to comply with that subsection; and

(b) as soon as practicable after the expiration of that period, comply or fully comply, as the case may be, with that subsection.

(3) A data user is not required to comply with subsection (1)(c) in any case where the disclosure concerned of the personal data to the third party consists of the third party's inspection of a register or other like document-

- (a) in which the data are entered or otherwise recorded; and
- (b) which is available for inspection by the public,

but this subsection shall not apply if the third party has been supplied with a copy, certified by or under the authority of the data user to be correct, of the data.

(Enacted 1995)

Section:	24	Circumstances in which data user shall or may refuse to comply with data correction request		30/06/1997
----------	----	---	--	------------

(1) Subject to subsection (2), a data user shall refuse to comply with section 23(1) in relation to a data correction request if the data user is not supplied with such information as the data user may reasonably require-

- (a) in order to satisfy the data user as to the identity of the requestor;
- (b) where the requestor purports to be a relevant person, in order to satisfy the data user-
 - (i) as to the identity of the individual in relation to whom the requestor purports to be such a person; and
 - (ii) that the requestor is such a person in relation to that individual.

(2) Subsection (1) shall not apply to a data correction request where the requestor is the same person as the requestor in respect of the data access request which gave rise to the data correction request.

(3) A data user may refuse to comply with section 23(1) in relation to a data correction request if-

- (a) the request is not in writing in the Chinese or English language;
- (b) the data user is not satisfied that the personal data to which the request relates are inaccurate;
- (c) the data user is not supplied with such information as the data user may reasonably require to ascertain in what way the personal data to which the request relates are inaccurate;
- (d) the data user is not satisfied that the correction which is the subject of the request is accurate; or
- (e) subject to subsection (4), any other data user controls the processing of the personal data to which the request relates in such a way as to prohibit the first-mentioned data user from complying (whether in whole or in part) with that section.

(4) Subsection (3)(e) shall not operate so as to excuse a data user from complying with section 23(1) in relation to the data correction request concerned to the extent that the data user can comply with that section without contravening the prohibition concerned.

(Enacted 1995)

Section:	25	Notification of refusal to comply with data correction request, etc.		30/06/1997
----------	----	--	--	------------

(1) A data user who pursuant to section 24 refuses to comply with section 23(1) in relation to a data correction request shall, as soon as practicable but, in any case, not later than 40 days after receiving the request, by notice in writing inform the requestor-

- (a) of the refusal and the reasons for the refusal; and
- (b) where section 24(3)(e) is applicable, of the name and address of the other data user concerned.

(2) Without prejudice to the generality of subsection (1), where-

- (a) the personal data to which a data correction request relates are an expression of opinion; and
- (b) the data user concerned is not satisfied that the opinion is inaccurate,

then the data user shall-

- (i) make a note, whether annexed to that data or elsewhere-
 - (A) of the matters in respect of which the opinion is considered by the requestor to be inaccurate; and
 - (B) in such a way that those data cannot be used by a person (including the data user and a third party) without the note being drawn to the attention of, and being available for inspection by, that person; and
- (ii) attach a copy of the note to the notice referred to in subsection (1) which relates to that request.

(3) In this section, "expression of opinion" (意見表達) includes an assertion of fact which-

- (a) is unverifiable; or
- (b) in all the circumstances of the case, is not practicable to verify.

(Enacted 1995)

Section:	26	Erasure of personal data no longer required	30/06/1997
----------	----	---	------------

- (1) A data user shall erase personal data held by the data user where the data are no longer required for the purpose (including any directly related purpose) for which the data were used unless-
- (a) any such erasure is prohibited under any law; or
 - (b) it is in the public interest (including historical interest) for the data not to be erased.
- (2) For the avoidance of doubt, it is hereby declared that-
- (a) a data user shall erase personal data in accordance with subsection (1) notwithstanding that any other data user controls (whether in whole or in part) the processing of the data;
 - (b) the first-mentioned data user shall not be liable in an action for damages at the suit of the second-mentioned data user in respect of any such erasure.

(Enacted 1995)

Section:	27	Log book to be kept by data user	30/06/1997
----------	----	----------------------------------	------------

- (1) A data user shall keep and maintain a log book-
- (a) for the purposes of this Part;
 - (b) in the Chinese or English language; and
 - (c) such that any particulars entered in the log book pursuant to this section are not erased therefrom before the expiration of-
 - (i) subject to subparagraph (ii), 4 years after the day on which they were so entered;
 - (ii) such longer or shorter period as may be prescribed, either generally or in any particular case, by regulations made under section 70.
- (2) A data user shall in accordance with subsection (3) enter in the log book-
- (a) where pursuant to section 20 the data user refuses to comply with a data access request, particulars of the reasons for the refusal;
 - (b) where pursuant to section 21(2) the data user does not comply with section 21(1), particulars of the prejudice that would be caused to the interest protected by the exemption concerned under Part VIII if the existence or non-existence of the personal data to which the data access request concerned relates were disclosed;
 - (c) where pursuant to section 24 the data user refuses to comply with section 23(1) in relation to a data correction request, particulars of the reasons for the refusal;
 - (d) any other particulars required by regulations made under section 70 to be entered in the log book.
- (3) The particulars required by subsection (2) to be entered by a data user in the log book shall be so entered-
- (a) in the case of particulars referred to in paragraph (a) of that subsection, on or before the notice under section 21(1) is served in respect of the refusal to which those particulars relate;
 - (b) in the case of particulars referred to in paragraph (b) of that subsection, on or before the notice under section 21(1) is served in respect of the refusal to which those particulars relate;
 - (c) in the case of particulars referred to in paragraph (c) of that subsection, on or before the notice under section 25(1) is served in respect of the refusal to which those particulars relate;
 - (d) in the case of particulars referred to in paragraph (d) of that subsection, within the period specified in regulations made under section 70 in respect of those particulars.
- (4) A data user shall-
- (a) permit the Commissioner to inspect and copy the log book (or any part thereof) at any reasonable time; and
 - (b) without charge, afford the Commissioner such facilities and assistance as the Commissioner may reasonably require for the purposes of such inspection and copying.

(Enacted 1995)

Section:	28	Imposition of fees by data user	30/06/1997
----------	----	---------------------------------	------------

- (1) A data user shall not impose a fee for complying or refusing to comply with a data access request or data correction request unless the imposition of the fee is expressly permitted by this section.
- (2) Subject to subsections (3) and (4), a data user may impose a fee for complying with a data access request.

(3) No fee imposed for complying with a data access request shall be excessive.

(4) Where pursuant to section 19(3)(c)(iv) or (v) or (4)(ii)(B)(II) a data user may comply with a data access request by supplying a copy of the personal data to which the request relates in one of 2 or more forms, the data user shall not, and irrespective of the form in which the data user complies with the request, impose a fee for complying with the request which is higher than the lowest fee the data user imposes for complying with the request in any of those forms.

(5) A data user may refuse to comply with a data access request unless and until any fee imposed by the data user for complying with the request has been paid.

(6) Where-

- (a) a data user has complied with a data access request by supplying a copy of the personal data to which the request relates; and
- (b) the data subject, or a relevant person on behalf of the data subject, requests the data user to supply a further copy of those data,

then the data user may, and notwithstanding the fee, if any, that the data user imposed for complying with that data access request, impose a fee for supplying that further copy which is not more than the administrative and other costs incurred by the data user in supplying that further copy.

(Enacted 1995)

Section:	29	Service and language of certain notices		30/06/1997
----------	----	---	--	------------

Without prejudice to the generality of section 68, where pursuant to a data access request or data correction request a data user is required to, or may, inform a requestor of any matter by notice in writing, then the requestor shall be deemed not to be so informed unless and until the requestor is served with the notice-

- (a) in the language in which the request is made if that language is Chinese or English;
- (b) in any other case, in the Chinese or English language as the data user thinks fit.

(Enacted 1995)

Section:	30	Matching procedure not to be carried out except with consent of data subject, etc.	L.N. 409 of 1997	01/08/1997
----------	----	--	------------------	------------

PART VI

MATCHING PROCEDURES AND TRANSFERS OF PERSONAL DATA, ETC.

(1) A data user shall not carry out, whether in whole or in part, a matching procedure-

- (a) unless and until each individual who is a data subject of the personal data the subject of that procedure has given his prescribed consent to the procedure being carried out;
- (b) unless and until the Commissioner has consented under section 32 to the procedure being carried out;
- (c) unless the procedure-
 - (i) belongs to a class of matching procedures specified in a notice under subsection (2); and
 - (ii) is carried out in accordance with the conditions, if any, specified in the notice; or
- (d) unless it is required or permitted under any provision of any Ordinance specified in Schedule 4.

(2) For the purposes of this section, the Commissioner may, by notice in the Gazette, specify-

- (a) a class of matching procedures;
- (b) subject to subsection (3), the conditions, if any, subject to which a matching procedure belonging to that class shall be carried out.

(3) The Commissioner shall, before specifying any conditions in a notice under subsection (2), consult with-

- (a) such bodies representative of data users to which the conditions will apply (whether in whole or in part); and
- (b) such other interested persons,

as he thinks fit.

(4) It is hereby declared that a notice under subsection (2) is subsidiary legislation.

(5) Subject to subsection (6), a data user shall not take adverse action against an individual in consequence (whether in whole or in part) of the carrying out of a matching procedure-

- (a) unless the data user has served a notice in writing on the individual-

- (i) specifying the adverse action it proposes to take and the reasons therefor; and
 - (ii) stating that the individual has 7 days after the receipt of the notice within which to show cause why that action should not be taken; and
- (b) until the expiration of those 7 days.

(6) Subsection (5) shall not operate to prevent a data user from taking adverse action against an individual if compliance with the requirements of that subsection would prejudice any investigation into the commission of an offence or the possible commission of an offence.

(Enacted 1995)

Section:	31	Matching procedure request		30/06/1997
----------	----	----------------------------	--	------------

- (1) A data user proposing to carry out, whether in whole or in part, a matching procedure may make a request-
- (a) in the specified form;
 - (b) to the Commissioner; and
 - (c) seeking the Commissioner's consent under section 32 to the carrying out of that procedure.

(2) Where 2 or more data users may each make a matching procedure request in respect of the same matching procedure, then any of those data users may make such a request on behalf of all those data users, and the provisions of this Ordinance (including subsection (1)) shall be construed accordingly.

(3) Without prejudice to the generality of subsection (2), it is hereby declared that a matching procedure request may be made in relation to 2 or more matching procedures, or a series of matching procedures, and the other provisions of this Ordinance (including section 32) shall be construed accordingly.

(Enacted 1995)

Section:	32	Determination of matching procedure request		30/06/1997
----------	----	---	--	------------

- (1) The Commissioner shall determine a matching procedure request-
- (a) not later than 45 days after receiving the request; and
 - (b) by taking into account the prescribed matters applicable to the request and-
 - (i) where he is satisfied as to those matters, serving a notice in writing on the requestor stating that he consents to the carrying out of the matching procedure to which the request relates subject to the conditions, if any, specified in the notice;
 - (ii) where he is not so satisfied, serving a notice in writing on the requestor stating-
 - (A) that he refuses to consent to the carrying out of the matching procedure to which the request relates; and
 - (B) such of those matters in respect of which he is not so satisfied and the reasons why he is not so satisfied.

(2) For the avoidance of doubt, it is hereby declared that a consent in a notice under subsection (1)(b)(i) to the carrying out of a matching procedure to which a matching procedure request relates shall not operate to prevent a data user who is neither the requestor nor, where section 31(2) applies to the request, any data user on whose behalf such request was made, from carrying out, whether in whole or in part, the procedure.

- (3) An appeal may be made to the Administrative Appeals Board-
- (a) against-
 - (i) any conditions specified in a notice under subsection (1) (b)(i); or
 - (ii) any refusal specified in a notice under subsection (1) (b)(ii); and
 - (b) by the requestor on whom the notice was served or any data user on whose behalf the matching procedure request concerned was made.

(4) In this section, "prescribed matter" (訂明事宜) means a matter specified in Schedule 5.

(Enacted 1995)

Section:	33	Prohibition against transfer of personal data to place outside Hong Kong except in specified circumstances		
----------	----	--	--	--

Remarks:
not yet in operation

(1) This section shall not apply to personal data other than personal data the collection, holding, processing or use of which-

- (a) takes place in Hong Kong; or
- (b) is controlled by a data user whose principal place of business is in Hong Kong.

(2) A data user shall not transfer personal data to a place outside Hong Kong unless-

- (a) the place is specified for the purposes of this section in a notice under subsection (3);
- (b) the user has reasonable grounds for believing that there is in force in that place any law which is substantially similar to, or serves the same purposes as, this Ordinance;
- (c) the data subject has consented in writing to the transfer;
- (d) the user has reasonable grounds for believing that, in all the circumstances of the case-
 - (i) the transfer is for the avoidance or mitigation of adverse action against the data subject;
 - (ii) it is not practicable to obtain the consent in writing of the data subject to that transfer; and
 - (iii) if it was practicable to obtain such consent, the data subject would give it;
- (e) the data are exempt from data protection principle 3 by virtue of an exemption under Part VIII; or
- (f) the user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not, in that place, be collected, held, processed or used in any manner which, if that place were Hong Kong, would be a contravention of a requirement under this Ordinance.

(3) Where the Commissioner has reasonable grounds for believing that there is in force in a place outside Hong Kong any law which is substantially similar to, or serves the same purposes as, this Ordinance, he may, by notice in the Gazette, specify that place for the purposes of this section.

(4) Where the Commissioner has reasonable grounds for believing that in a place specified in a notice under subsection (3) there is no longer in force any law which is substantially similar to, or serves the same purposes as, this Ordinance, he shall, either by repealing or amending that notice, cause that place to cease to be specified for the purposes of this section.

(5) For the avoidance of doubt, it is hereby declared that-

- (a) for the purposes of subsection (1)(b), a data user which is a company incorporated in Hong Kong is a data user whose principal place of business is in Hong Kong;
- (b) a notice under subsection (3) is subsidiary legislation; and
- (c) this section shall not operate to prejudice the generality of section 50.

(Enacted 1995)

Section:	34	Use of personal data in direct marketing	30/06/1997
----------	----	--	------------

(1) A data user who-

- (a) has obtained personal data from any source (including the data subject); and
- (b) uses the data for direct marketing purposes,

shall-

- (i) the first time he so uses those data after this section comes into operation, inform the data subject that the data user is required, without charge to the data subject, to cease to so use those data if the data subject so requests;
- (ii) if the data subject so requests, cease to so use those data without charge to the data subject.

(2) In this section-

"direct marketing" (直接促銷) means-

- (a) the offering of goods, facilities or services;
- (b) the advertising of the availability of goods, facilities or services; or
- (c) the solicitation of donations or contributions for charitable, cultural, philanthropic, recreational, political or other purposes,

by means of-

- (i) information or goods sent to any person by mail, facsimile transmission, electronic mail, or other similar means of communication, where the information or goods are addressed to a specific person or specific persons by name; or
- (ii) telephone calls made to specific persons.

(Enacted 1995)

Section:	35	Repeated collections of personal data in same circumstances		30/06/1997
----------	----	---	--	------------

- (1) A data user who-
- (a) has complied with the provisions of data protection principle 1(3) in respect of the collection of any personal data from the data subject ("first collection"); and
 - (b) on any subsequent occasion again collects personal data from the data subject ("subsequent collection"),
- is not required to comply with those provisions in respect of the subsequent collection if, but only if-
- (i) to comply with those provisions in respect of that subsequent collection would be to repeat, without any material difference, what was done to comply with that principle in respect of the first collection; and
 - (ii) not more than 12 months have elapsed between the first collection and the subsequent collection.
- (2) For the avoidance of doubt, it is hereby declared that subsection (1) shall not operate to prevent a subsequent collection from becoming a first collection if, but only if, the data user concerned has complied with the provisions of data protection principle 1(3) in respect of the subsequent collection.
- (Enacted 1995)

Section:	36	Inspections of personal data systems		30/06/1997
----------	----	--------------------------------------	--	------------

PART VII

INSPECTIONS, COMPLAINTS AND INVESTIGATIONS

- Without prejudice to the generality of section 38, the Commissioner may carry out an inspection of-
- (a) any personal data system used by a data user; or
 - (b) any personal data system used by a data user belonging to a class of data users,
- for the purposes of ascertaining information to assist the Commissioner in making recommendations-
- (i) to-
 - (A) where paragraph (a) is applicable, the relevant data user;
 - (B) where paragraph (b) is applicable, the class of data users to which the relevant data user belongs;
 and
 - (ii) relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the relevant data user, or the class of data users to which the relevant data user belongs, as the case may be.
- (Enacted 1995)

Section:	37	Complaints		30/06/1997
----------	----	------------	--	------------

- (1) An individual, or a relevant person on behalf of an individual, may make a complaint to the Commissioner about an act or practice-
- (a) specified in the complaint; and
 - (b) that-
 - (i) has been done or engaged in, or is being done or engaged in, as the case may be, by a data user specified in the complaint;
 - (ii) relates to personal data of which the individual is or, in any case in which the data user is relying upon an exemption under Part VIII, may be, the data subject; and
 - (iii) may be a contravention of a requirement under this Ordinance (including section 28(4)).
- (2) Where 2 or more individuals may each make a complaint about the same act or practice, then any of those individuals, or any relevant person on behalf of any of those individuals, may make such a complaint on behalf of all those individuals, and the provisions of this Ordinance (including subsection (1)) shall be construed accordingly.
- (3) A complaint shall be-
- (a) in writing in the Chinese or English language; or
 - (b) in such other form as the Commissioner may accept.
- (4) It shall be the duty of the Commissioner and each prescribed officer who has been employed under section 9(1)(a) to provide appropriate assistance to an individual, or a relevant person on behalf of an individual, who wishes

to make a complaint and requires assistance to formulate the complaint.

(Enacted 1995)

Section:	38	Investigations by Commissioner		30/06/1997
----------	----	--------------------------------	--	------------

Where the Commissioner-

- (a) receives a complaint; or
- (b) has reasonable grounds to believe that an act or practice-
 - (i) has been done or engaged in, or is being done or engaged in, as the case may be, by a data user;
 - (ii) relates to personal data; and
 - (iii) may be a contravention of a requirement under this Ordinance,

then-

- (i) where paragraph (a) is applicable, the Commissioner shall, subject to section 39, carry out an investigation in relation to the relevant data user to ascertain whether the act or practice specified in the complaint is a contravention of a requirement under this Ordinance;
- (ii) where paragraph (b) is applicable, the Commissioner may carry out an investigation in relation to the relevant data user to ascertain whether the act or practice referred to in that paragraph is a contravention of a requirement under this Ordinance.

(Enacted 1995)

Section:	39	Restrictions on investigations initiated by complaints		30/06/1997
----------	----	--	--	------------

(1) Notwithstanding the generality of the powers conferred on the Commissioner by this Ordinance, the Commissioner may refuse to carry out or continue an investigation initiated by a complaint if-

- (a) the complainant (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person) has had actual knowledge of the act or practice specified in the complaint for more than 2 years immediately preceding the date on which the Commissioner received the complaint, unless the Commissioner is satisfied that in all the circumstances of the case it is proper to carry out or continue, as the case may be, the investigation;
- (b) the complaint is made anonymously;
- (c) the complainant cannot be identified or traced;
- (d) none of the following conditions is fulfilled in respect of the act or practice specified in the complaint-
 - (i) either-
 - (A) the complainant (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person) was resident in Hong Kong; or
 - (B) the relevant data user was able to control, in or from Hong Kong, the collection, holding, processing or use of the personal data concerned, at any time the act or practice was done or engaged in, as the case may be;
 - (ii) the complainant (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person) was in Hong Kong at any time the act or practice was done or engaged in, as the case may be;
 - (iii) in the opinion of the Commissioner, the act or practice done or engaged in, as the case may be, may prejudice the enforcement of any right, or the exercise of any privilege, acquired or accrued in Hong Kong by the complainant (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person); or
- (e) the Commissioner is satisfied that the relevant data user has not been a data user for a period of not less than 2 years immediately preceding the date on which the Commissioner received the complaint.

(2) The Commissioner may refuse to carry out or continue an investigation initiated by a complaint if he is of the opinion that, having regard to all the circumstances of the case-

- (a) the complaint, or a complaint of a substantially similar nature, has previously initiated an investigation as a result of which the Commissioner was of the opinion that there had been no contravention of a requirement under this Ordinance;
- (b) the act or practice specified in the complaint is trivial;
- (c) the complaint is frivolous or vexatious or is not made in good faith; or
- (d) any investigation or further investigation is for any other reason unnecessary.

(3) Where the Commissioner refuses under this section to carry out or continue an investigation initiated by a complaint, he shall, as soon as practicable but, in any case, not later than 45 days after receiving the complaint, by notice in writing served on the complainant accompanied by a copy of subsection (4), inform the complainant-

- (a) of the refusal; and
- (b) of the reasons for the refusal.

(4) An appeal may be made to the Administrative Appeals Board-

- (a) against any refusal specified in a notice under subsection (3); and
- (b) by the complainant on whom the notice was served (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person, or either).

(Enacted 1995)

Section:	40	Commissioner may carry out or continue investigation initiated by complaint notwithstanding withdrawal of complaint		30/06/1997
----------	----	---	--	------------

Where the Commissioner is of the opinion that it is in the public interest so to do, he may carry out or continue an investigation initiated by a complaint notwithstanding that the complainant has withdrawn the complaint and, in any such case, the provisions of this Ordinance shall apply to the complaint and the complainant as if the complaint had not been withdrawn.

(Enacted 1995)

Section:	41	Commissioner to inform relevant data user of inspection or investigation		30/06/1997
----------	----	--	--	------------

(1) The Commissioner shall, before carrying out an inspection or, subject to subsection (2), an investigation, by notice in writing served on the relevant data user, inform the data user of his intention to carry out the inspection or investigation, as the case may be.

(2) The Commissioner is not required to comply with subsection (1) in the case of any investigation in respect of which he has reasonable grounds to believe that to so comply may prejudice the purposes of the investigation.

(Enacted 1995)

Section:	42	Power of entry on premises for the purposes of an inspection or investigation		30/06/1997
----------	----	---	--	------------

(1) Subject to subsections (3) and (8), the Commissioner may, for the purposes of an inspection-

- (a) where the personal data system, or any part thereof, the subject of the inspection is situated in-
 - (i) non-domestic premises, enter the premises at any reasonable time;
 - (ii) domestic premises, enter the premises with the consent of any person (other than a minor) resident therein;
- (b) carry out in the premises the inspection.

(2) Subject to subsections (3) and (8), the Commissioner may, for the purposes of an investigation-

- (a) enter any premises-
 - (i) occupied by the relevant data user; or
 - (ii) in which is situated the personal data system, or any part thereof, used by the relevant data user;
- (b) carry out in the premises the investigation.

(3) Subject to subsections (4) and (5), the Commissioner shall, not less than 14 days before exercising his power under subsection (1) or (2) in respect of any premises, by notice in writing served on the relevant data user, inform the data user-

- (a) of the premises in respect of which he proposes to exercise that power; and
- (b) that the power will not be so exercised before the expiration of 14 days after service of the notice.

(4) Without prejudice to the generality of subsection (5), where any domestic premises are specified in a notice under subsection (3) in respect of which the Commissioner proposes to exercise his power under subsection (2), then the Commissioner shall not exercise that power in respect of those premises unless and until a person (other than a minor) resident therein consents thereto before the expiration of 14 days after service of the notice.

(5) The Commissioner may, pursuant to a warrant issued under subsection (6), exercise his power under

subsection (2) in respect of the premises specified in the warrant without complying with subsection (3).

(6) A magistrate may, if satisfied by information upon oath by the Commissioner or any prescribed officer that there are reasonable grounds for believing that the purposes of any investigation may be substantially prejudiced if the Commissioner were required to comply with subsection (3) before exercising his power under subsection (2) in respect of any premises, issue a warrant-

- (a) in the form specified in Part 1 of Schedule 6; and
- (b) in respect of those premises.

(7) A magistrate may, if satisfied by information upon oath by the Commissioner or any prescribed officer that there are reasonable grounds for believing that the purposes of an investigation may be substantially prejudiced if the Commissioner is prevented by the operation of subsection (4) from exercising his power under subsection (2) in respect of any domestic premises, issue a warrant-

- (a) in the form specified in Part 2 of Schedule 6; and
- (b) authorizing the Commissioner to exercise that power in respect of those premises.

(8) The Commissioner shall not exercise his power under subsection (1) or (2) in respect of any premises in such a way as to unduly disrupt any operations being carried out in the premises, whether by the relevant data user or any other person.

(9) Where the Commissioner exercises his power under subsection (1) or (2), the relevant data user shall, without charge, afford the Commissioner such facilities and assistance as the Commissioner may reasonably require for the purposes of the inspection or investigation concerned.

(10) Where the Commissioner, pursuant to a warrant issued under subsection (6), exercises his power under subsection (2) in respect of the premises specified in the warrant, he shall produce the warrant for inspection by any person found in those premises who questions his authority to exercise that power in respect of those premises.

(11) In this section and Schedule 6-

"domestic premises" (住宅處所) means any premises which are constructed or intended to be used for habitation;

"non-domestic premises" (非住宅處所) means any premises other than domestic premises;

"premises" (處所) means-

- (a) any building where no part of the building is separately occupied, and includes any land appertaining to the building;
- (b) in any other case, any part of a building which is separately occupied, and includes any land appertaining to such part.

(Enacted 1995)

Section:	43	Proceedings of Commissioner	30/06/1997
----------	----	-----------------------------	------------

(1) Subject to the provisions of this Ordinance, the Commissioner may, for the purposes of any investigation-

- (a) be furnished with any information, document or thing, from such persons, and make such inquiries, as he thinks fit; and
- (b) regulate his procedure in such manner as he thinks fit.

(2) Any hearing for the purposes of an investigation shall be carried out in public unless-

- (a) the Commissioner is of the opinion that, in all the circumstances of the case, the investigation should be carried out in private; or
- (b) if the investigation was initiated by a complaint, the complainant requests in writing that the investigation be carried out in private.

(3) Counsel and solicitors shall not have any right of audience before the Commissioner at any hearing for the purposes of an investigation, but may appear before him if he thinks fit.

(4) It shall not be necessary for the Commissioner to hold any hearing for the purposes of an investigation and no person shall be entitled to be heard by the Commissioner.

(5) If at any time during the course of an investigation it appears to the Commissioner that there may be sufficient grounds for him to make any report or recommendation that may criticize or adversely affect any person he shall give to the person an opportunity to be heard.

(Enacted 1995)

Section:	44	Evidence	25 of 1998 s. 2	01/07/1997
----------	----	----------	-----------------	------------

Remarks:

Amendments retroactively made-see 25 of 1998 s. 2

(1) Subject to subsection (2) and section 45, the Commissioner may, for the purposes of any investigation, summon before him any person who-

- (a) in the opinion of the Commissioner, is able to give any information relevant to those purposes;
- (b) where the investigation was initiated by a complaint, is the complainant (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person, or both),

and may examine any such person and require him to furnish to the Commissioner any information and to produce any document or thing which, in the opinion of the Commissioner, is relevant to those purposes and which may be in the possession or under the control of any such person.

(2) Where-

- (a) an investigation has been initiated by a complaint;
- (b) the complaint relates, whether in whole or in part, to personal data referred to in section 61(1);
- (c) the Commissioner has, for the purposes of that investigation, under subsection (1)(a) summoned before him a person; and
- (d) that person asserts, in response to any requirement under subsection (1) by the Commissioner to furnish him with information or to produce a document or thing, that-
 - (i) to comply with that requirement would directly or indirectly disclose the identity of the individual from whom those data were collected (whether in whole or in part); or
 - (ii) he is not required to comply with that requirement by virtue of any common law privilege,

then-

- (i) notwithstanding any other provision of this Ordinance, the Commissioner shall not serve an enforcement notice on that person in relation to that requirement;
- (ii) the Commissioner may, not later than 28 days after that assertion is made known to him, make an application to the Court of First Instance for an order directing that person to comply with that requirement; (Amended 25 of 1998 s. 2)
- (iii) the Court of First Instance may make the order if, but only if, it is satisfied, having regard to all the circumstances (including the circumstances of the complainant), that- (Amended 25 of 1998 s. 2)
 - (A) if the act or practice specified in the complaint were proven to be a contravention of a requirement under this Ordinance, the contravention would be of sufficient gravity to warrant that person complying with the requirement referred to in paragraph (d);
 - (B) that investigation would be substantially prejudiced if the requirement referred to in paragraph (d) were not complied with;
 - (C) it is in the public interest, having regard to the benefit likely to accrue to that investigation, that the requirement referred to in paragraph (d) be complied with; and
 - (D) in any case to which paragraph (d)(ii) is applicable, the common law privilege asserted does not apply; and
- (iv) on the hearing of the application, the Commissioner, that person and the complainant shall each be entitled to be heard on the application and to call, examine and cross-examine any witness.

(3) Where-

- (a) a person has complied with a requirement referred to in subsection (2)(d) the subject of an assertion referred to in that subsection; and
- (b) the result (whether in whole or in part) of the investigation to which that requirement relates is that the Commissioner is of the opinion that the individual concerned referred to in subsection (2)(d)(i) has not contravened a requirement under this Ordinance in relation to the matter the subject of the complaint which initiated the investigation,

then, notwithstanding any other provision of this Ordinance, neither the Commissioner nor any prescribed officer shall disclose the identity of that individual to the complainant.

(4) The Court of First Instance may, of its own volition or on an application made to it for the purpose, by order reverse, vary or discharge an order made under subsection (2)(iii) or suspend the operation of such an order. (Amended 25 of 1998 s. 2)

(5) Provision may be made by rules of court-

- (a) with respect to applications to the Court of First Instance under subsection (2)(iii) or (4);
- (b) generally with respect to procedure before the Court of First Instance in relation to any such application. (Amended 25 of 1998 s. 2)
- (6) Subsection (5) is without prejudice to the generality of any existing power to make rules.
- (7) The Commissioner may administer an oath for the purposes of an examination under subsection (1) if he thinks fit.
- (8) It is hereby declared that-
 - (a) no obligation to maintain secrecy or other restriction, imposed by law, upon the disclosure of any information, document or other thing, that is or has been in the possession or under the control of any person referred to in subsection (1), shall apply to its disclosure for the purposes of an investigation; and
 - (b) any requirement by the Commissioner that any such information, document or thing as is referred to in paragraph (a) be disclosed or produced for the purposes of an investigation shall be sufficient authority for its disclosure or production to the Commissioner.
- (9) The Commissioner may pay the reasonable expenses of complainants (including, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person) and witnesses incurred during the course of an investigation.

(Enacted 1995)

Section:	45	Protection of witnesses, etc.	25 of 1998; 34 of 1999	01/07/1997
----------	----	-------------------------------	------------------------	------------

Remarks:

Adaptation amendments retroactively made - see 25 of 1998 s. 2; 34 of 1999 s. 3

(1) Every person shall have the same privileges in relation to the giving of information, the answering of questions, and the production of documents and things, for the purposes of an investigation, as witnesses have in civil proceedings in the High Court but any rule of law which authorizes or requires the withholding of any document or thing, or the refusal to answer any question, on the ground that the disclosure of the document or thing or the answering of the question, as the case may be, would be injurious to the public interest, shall not apply in respect of any investigation. (Amended 25 of 1998 s. 2)

(2) Except on the trial of any person for perjury in respect of his sworn testimony, or for an offence under this Ordinance, no statement made or answer given by that or any other person in the course of any investigation shall be admissible in evidence against any person, before any magistrate or in any court or at any inquiry or in any other proceedings, and no evidence in respect of an investigation shall be given against any person.

(3) Where the giving of any information or the answering of any question or the production of any document or thing would involve the disclosure, without the consent of the Chief Executive, of the deliberations of the Executive Council, the Commissioner shall not require the information or answer to be given or, as the case may be, the document or thing to be produced. (Amended 34 of 1999 s. 3)

(Enacted 1995)

Section:	46	Commissioner, etc. to maintain secrecy		30/06/1997
----------	----	--	--	------------

(1) Subject to subsections (2) and (3), the Commissioner and every prescribed officer shall maintain secrecy in respect of all matters that come to their actual knowledge in the performance of their functions and the exercise of their powers under this Part.

(2) Subsection (1) shall not operate so as to prevent the Commissioner or any prescribed officer from-

- (a) disclosing in the course of proceedings-
 - (i) for an offence under this Ordinance; and
 - (ii) before any court or magistrate, any matter relevant to those proceedings;
- (b) reporting evidence of any crime to such authority as he considers appropriate;
- (c) disclosing to a person any matter referred to in subsection (1) which, in the opinion of the Commissioner or prescribed officer, may be ground for a complaint by that person.

(3) Subject to subsection (4), the Commissioner may disclose in any report made by him under this Ordinance

any matter that in his opinion ought to be disclosed in order to establish grounds for his findings and recommendations other than a matter the disclosure of which in his opinion would involve the disclosure of personal data that are exempt from data protection principle 6 by virtue of an exemption under Part VIII.

(4) The Commissioner shall not publish a report under this Ordinance after completing an inspection or investigation unless-

- (a) a copy of the report in the form in which it is to be published has been supplied to the relevant data user;
- (b) that copy is accompanied by a notice in writing inviting the data user to advise the Commissioner, in writing and not later than 28 days after being served with the copy, whether-
 - (i) in the opinion of the data user there is any matter in the copy the disclosure of which would involve the disclosure of personal data that are exempt from the provisions of data protection principle 6 by virtue of an exemption under Part VIII; and
 - (ii) the data user objects to the disclosure of the matter; and
- (c) either-
 - (i) the period referred to in paragraph (b) has expired without the Commissioner receiving any such advice; or
 - (ii) such advice is received by the Commissioner and-
 - (A) the Commissioner deletes from the report the matter the subject of the advice; or
 - (B) the Commissioner decides not to delete that matter from the report and-
 - (I) the period referred to in subsection (6) expires without the data user making an appeal under that subsection against that decision; or
 - (II) such an appeal is unsuccessful or withdrawn.

(5) Where the Commissioner makes a decision referred to in subsection (4)(c)(ii)(B), he shall serve on the relevant data user who gave the advice concerned a notice in writing-

- (a) stating his decision;
- (b) informing the data user that he may appeal under subsection (6) against that decision; and
- (c) accompanied by a copy of this section.

(6) An appeal may be made to the Administrative Appeals Board against a decision of the Commissioner referred to in subsection (4)(c)(ii)(B) by the relevant data user not later than 14 days after the notice under subsection (5) stating that decision has been served on the data user.

(Enacted 1995)

Section:	47	Persons to be informed of result of inspection or investigation	30/06/1997
----------	----	---	------------

(1) Where the Commissioner has completed an inspection, he shall, in such manner and at such time as he thinks fit, inform the relevant data user of-

- (a) the result of the inspection;
- (b) any recommendations arising from the inspection that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the data user;
- (c) any report arising from the inspection that he proposes to publish under section 48; and
- (d) such other comments arising from the inspection as he thinks fit to make.

(2) Where the Commissioner has completed an investigation, he shall, in such manner and at such time as he thinks fit, inform the relevant data user of-

- (a) the result of the investigation;
- (b) any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the data user;
- (c) any report arising from the investigation that he proposes to publish under section 48;
- (d) whether or not he proposes to serve an enforcement notice on the data user in consequence of the investigation; and
- (e) such other comments arising from the investigation as he thinks fit to make.

(3) Where the Commissioner has completed an investigation initiated by a complaint, he shall, in such manner and at such time as he thinks fit, inform the complainant of-

- (a) the result of the investigation;

- (b) any recommendations made to the relevant data user under subsection (2)(b);
- (c) any report arising from the investigation that he proposes to publish under section 48;
- (d) any comments made by or on behalf of the relevant data user on any such recommendations or report;
- (e) whether or not he has served, or proposes to serve, an enforcement notice on the relevant data user in consequence of the investigation;
- (f) if the Commissioner has not so served, and does not propose to so serve, such enforcement notice, his right to object thereto under subsection (4); and
- (g) such other comments arising from the investigation as he thinks fit to make.

(4) The complainant (or, if the complainant is a relevant person, the individual in respect of whom the complainant is such a person, or either) may appeal to the Administrative Appeals Board against a decision of the Commissioner-

- (a) to the effect that he has not served, and does not propose to serve, an enforcement notice on the relevant data user in consequence of the investigation concerned; and
- (b) of which the complainant was informed in the notice concerned under subsection (3) served on him.

(Enacted 1995)

Section:	48	Reports by Commissioner		30/06/1997
----------	----	-------------------------	--	------------

(1) Subject to subsection (3), the Commissioner may, after completing an inspection where section 36(b) is applicable, publish a report-

- (a) setting out any recommendations arising from the inspection that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and
- (b) in such manner as he thinks fit.

(2) Subject to subsection (3), the Commissioner may, after completing an investigation and if he is of the opinion that it is in the public interest to do so, publish a report-

- (a) setting out-
 - (i) the result of the investigation;
 - (ii) any recommendations arising from the investigation that the Commissioner thinks fit to make relating to the promotion of compliance with the provisions of this Ordinance, in particular the data protection principles, by the class of data users to which the relevant data user belongs; and
 - (iii) such other comments arising from the investigation as he thinks fit to make; and
- (b) in such manner as he thinks fit.

(3) Subject to subsection (4), a report published under subsection (1) or (2) shall be so framed as to prevent the identity of any individual being ascertained from it.

(4) Subsection (3) shall not apply to any individual who is-

- (a) the Commissioner or a prescribed officer;
- (b) the relevant data user.

(Enacted 1995)

Section:	49	Cases in which sections 47 and 48 shall not apply		30/06/1997
----------	----	---	--	------------

Where-

- (a) the Commissioner has completed an investigation (and whether or not the investigation was initiated by a complaint);
- (b) the result of the investigation is that the act or practice the subject of the investigation is not a contravention of a requirement under this Ordinance because of an exemption under Part VIII; and
- (c) the interest protected by that exemption would be likely to be prejudiced if sections 47 and 48 applied in relation to the investigation,

then-

- (i) those sections shall not apply in relation to the investigation; and
- (ii) the Commissioner shall, in such manner and at such time as he thinks fit-
 - (A) inform the relevant data user of the result of the investigation and such other comments arising from the investigation as he thinks fit;
 - (B) if the investigation was initiated by a complaint, inform the complainant that the result of the

investigation is that he is satisfied that the act or practice the subject of the investigation is not a contravention of a requirement under this Ordinance (or words to the like effect).

(Enacted 1995)

Section:	50	Enforcement notices		30/06/1997
----------	----	---------------------	--	------------

(1) Where, following the completion of an investigation, the Commissioner is of the opinion that the relevant data user-

- (a) is contravening a requirement under this Ordinance; or
- (b) has contravened such a requirement in circumstances that make it likely that the contravention will continue or be repeated,

then the Commissioner may serve on the relevant data user a notice in writing-

- (i) stating that he is of that opinion;
- (ii) specifying the requirement as to which he is of that opinion and the reasons why he is of that opinion;
- (iii) directing the data user to take such steps as are specified in the notice to remedy the contravention or, as the case may be, the matters occasioning it within such period (ending not earlier than the period specified in subsection (7) within which an appeal against the notice may be made) as is specified in the notice; and
- (iv) accompanied by a copy of this section.

(2) In deciding whether to serve an enforcement notice the Commissioner shall consider whether the contravention or matter to which the notice relates has caused or is likely to cause damage or distress to any individual who is the data subject of any personal data to which the contravention or matter, as the case may be, relates.

(3) The steps specified in an enforcement notice to remedy any contravention or matter to which the notice relates may be framed-

- (a) to any extent by reference to any approved code of practice;
- (b) so as to afford the relevant data user a choice between different ways of remedying the contravention or matter, as the case may be.

(4) Subject to subsection (5), the period specified in an enforcement notice for taking the steps specified in it shall not expire before the end of the period specified in subsection (7) within which an appeal against the notice may be made and, if such an appeal is made, those steps need not be taken pending the determination or withdrawal of the appeal.

(5) If the Commissioner is of the opinion that by reason of special circumstances the steps specified in an enforcement notice should be taken as a matter of urgency-

- (a) he may include a statement to that effect in the notice together with the reasons why he is of that opinion;
- (b) where such a statement is so included, subsection (4) shall not apply but the notice shall not require those steps to be taken before the end of the period of 7 days beginning with the date on which the notice was served.

(6) The Commissioner may cancel an enforcement notice by notice in writing served on the relevant data user.

(7) An appeal may be made to the Administrative Appeals Board against an enforcement notice by the relevant data user not later than 14 days after the notice was served.

(8) Where the Commissioner-

- (a) forms an opinion referred to in subsection (1) in respect of the relevant data user at any time before the completion of an investigation; and
- (b) is also of the opinion that, by reason of special circumstances, an enforcement notice should be served on the relevant data user as a matter of urgency,

he may so serve such notice notwithstanding that the investigation has not been completed and, in any such case-

- (i) the Commissioner shall, without prejudice to any other matters to be included in such notice, specify in the notice the reasons as to why he is of the opinion referred to in paragraph (b); and
- (ii) the other provisions of this Ordinance (including this section) shall be construed accordingly.

(Enacted 1995)

Section:	51	Interpretation		30/06/1997
----------	----	----------------	--	------------

PART VIII

EXEMPTIONS

Where any personal data are exempt from any provision of this Ordinance by virtue of this Part, then, in respect of those data and to the extent of that exemption, that provision neither confers any right nor imposes any requirement on any person, and the other provisions of this Ordinance which relate (whether directly or indirectly) to that provision shall be construed accordingly.

(Enacted 1995)

Section:	52	Domestic purposes		30/06/1997
----------	----	-------------------	--	------------

Personal data held by an individual and-

- (a) concerned only with the management of his personal, family or household affairs; or
- (b) so held only for recreational purposes,

are exempt from the provisions of the data protection principles, Parts IV and V and sections 36 and 38(b).

(Enacted 1995)

Section:	53	Employment - staff planning		30/06/1997
----------	----	-----------------------------	--	------------

Personal data which consist of information relevant to any staff planning proposal to-

- (a) fill any series of positions of employment which are presently, or may become, unfilled; or
- (b) cease any group of individuals' employment,

are exempt from the provisions of data protection principle 6 and section 18(1)(b).

(Enacted 1995)

Section:	54	Employment - transitional provisions		30/06/1997
----------	----	--------------------------------------	--	------------

(1) Personal data-

- (a) held by a data user-
 - (i) immediately before the appointed day;
 - (ii) who is the employer of the data subject; and
 - (iii) relating to the employment of the subject; and
- (b) provided by an individual on the implicit or explicit condition that the subject would not have access to the data,

are exempt from the provisions of data protection principle 6 and section 18(1)(b) until the expiration of 7 years immediately following the enactment of this Ordinance.

(2) Personal data-

- (a) to which subsection (1)(a) applies; or
- (b) held by a data user-
 - (i) but not so held at any time before the appointed day;
 - (ii) who is the employer of the data subject; and
 - (iii) relating to the employment of the subject,

are exempt from the provisions of data protection principle 6 and section 18(1)(b) until 1 July 1996.

(Enacted 1995)

Section:	55	Relevant process		30/06/1997
----------	----	------------------	--	------------

(1) Personal data the subject of a relevant process are exempt from the provisions of data protection principle 6 and section 18(1)(b) until the completion of that process.

(2) In this section-

"completion" (完成), in relation to a relevant process, means the making of the determination concerned referred to in paragraph (a) of the definition of "relevant process";

"relevant process" (有關程序)-

- (a) subject to paragraph (b), means any process whereby personal data are considered by one or more

persons for the purpose of determining, or enabling there to be determined-

- (i) the suitability, eligibility or qualifications of the data subject for-
 - (A) employment or appointment to office;
 - (B) promotion in employment or office or continuance in employment or office;
 - (C) removal from employment or office; or
 - (D) the awarding of contracts, awards (including academic and professional qualifications), scholarships, honours or other benefits;
- (ii) whether any contract, award (including academic and professional qualifications), scholarship, honour or benefit relating to the data subject should be continued, modified or cancelled; or
- (iii) whether any disciplinary action should be taken against the data subject for a breach of the terms of his employment or appointment to office;
- (b) does not include any such process where no appeal, whether under an Ordinance or otherwise, may be made against any such determination.

(Enacted 1995)

Section:	56	Personal references		30/06/1997
----------	----	---------------------	--	------------

Personal data held by a data user which consist of a personal reference-

- (a) given by an individual other than in the ordinary course of his occupation; and
- (b) relevant to another individual's suitability or otherwise to fill any position of employment or office which is presently, or may become, unfilled,

are exempt from the provisions of data protection principle 6 and section 18(1)(b)-

- (i) in any case, unless the individual referred to in paragraph (a) has informed the data user in writing that he has no objection to the reference being seen by the individual referred to in paragraph (b) (or words to the like effect); or
- (ii) in the case of a reference given on or after the day on which this section comes into operation, until the individual referred to in paragraph (b) has been informed in writing that he has been accepted or rejected to fill that position or office (or words to the like effect),

whichever first occurs.

(Enacted 1995)

Section:	57	Security, etc. in respect of Hong Kong	L.N. 362 of 1997; 34 of 1999	01/07/1997
----------	----	--	---------------------------------	------------

Remarks:

Adaptation amendments retroactively made - see 34 of 1999 s. 3

(1) Personal data held by or on behalf of the Government for the purposes of safeguarding security, defence or international relations in respect of Hong Kong are exempt from the provisions of data protection principle 6 and section 18(1)(b) where the application of those provisions to the data would be likely to prejudice any of the matters referred to in this subsection.

(2) Personal data are exempt from the provisions of data protection principle 3 in any case in which-

- (a) the use of the data is for any of the purposes referred to in subsection (1) (and whether or not the data are held for any of those purposes); and
- (b) the application of those provisions in relation to such use would be likely to prejudice any of the matters referred to in that subsection,

and in any proceedings against any person for a contravention of any of those provisions it shall be a defence to show that he had reasonable grounds for believing that failure to so use the data would have been likely to prejudice any of those matters.

(3) Any question whether an exemption under subsection (1) is or at any time was required in respect of any personal data may be determined by the Chief Executive or Chief Secretary for Administration; and a certificate signed by the Chief Executive or Chief Secretary for Administration certifying that the exemption is or at any time was so required shall be evidence of that fact. (Amended L.N. 362 of 1997; 34 of 1999 s. 3)

(4) For the purposes of subsection (2), a certificate signed by the Chief Executive or Chief Secretary for Administration certifying that personal data are or have been used for any purpose referred to in subsection (1) shall

be evidence of that fact. (Amended L.N. 362 of 1997; 34 of 1999 s. 3)

(5) The Chief Executive or Chief Secretary for Administration may, in a certificate referred to in subsection (3) or (4), in respect of the personal data to which the certificate relates and for the reasons specified in that certificate, direct the Commissioner not to carry out an inspection or investigation and, in any such case, the Commissioner shall comply with the direction. (Amended L.N. 362 of 1997; 34 of 1999 s. 3)

(6) A document purporting to be a certificate referred to in subsection (3) or (4) shall be received in evidence and, in the absence of evidence to the contrary, shall be deemed to be such a certificate.

(7) In this section-

"international relations" (國際關係) includes relations with any international organization;

"security" (保安) includes the prevention or preclusion of persons (including persons detained in accordance with the provisions of the Immigration Ordinance (Cap 115)) entering and remaining in Hong Kong who do not have the right to enter and remain in Hong Kong.

(Enacted 1995)

Section:	58	Crime, etc.	L.N. 28 of 2010	12/03/2010
----------	----	-------------	-----------------	------------

(1) Personal data held for the purposes of-

- (a) the prevention or detection of crime;
- (b) the apprehension, prosecution or detention of offenders;
- (c) the assessment or collection of any tax or duty;
- (d) the prevention, preclusion or remedying (including punishment) of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;
- (e) the prevention or preclusion of significant financial loss arising from-
 - (i) any imprudent business practices or activities of persons; or
 - (ii) unlawful or seriously improper conduct, or dishonesty or malpractice, by persons;
- (f) ascertaining whether the character or activities of the data subject are likely to have a significantly adverse impact on any thing-
 - (i) to which the discharge of statutory functions by the data user relates; or
 - (ii) which relates to the discharge of functions to which this paragraph applies by virtue of subsection (3); or

(g) discharging functions to which this paragraph applies by virtue of subsection (3), are exempt from the provisions of data protection principle 6 and section 18(1)(b) where the application of those provisions to the data would be likely to-

- (i) prejudice any of the matters referred to in this subsection; or
- (ii) directly or indirectly identify the person who is the source of the data.

(1A) In subsection (1)(c), "tax" (稅項) includes any tax of a territory outside Hong Kong if-

- (a) arrangements having effect under section 49(1A) of the Inland Revenue Ordinance (Cap 112) are made with the government of that territory; and
- (b) that tax is the subject of a provision of the arrangements that requires disclosure of information concerning tax of that territory. (Added 1 of 2010 s. 9)

(2) Personal data are exempt from the provisions of data protection principle 3 in any case in which-

- (a) the use of the data is for any of the purposes referred to in subsection (1) (and whether or not the data are held for any of those purposes); and
- (b) the application of those provisions in relation to such use would be likely to prejudice any of the matters referred to in that subsection,

and in any proceedings against any person for a contravention of any of those provisions it shall be a defence to show that he had reasonable grounds for believing that failure to so use the data would have been likely to prejudice any of those matters.

(3) Paragraphs (f)(ii) and (g) of subsection (1) apply to any functions of a financial regulator-

- (a) for protecting members of the public against financial loss arising from-
 - (i) dishonesty, incompetence, malpractice or seriously improper conduct by persons-
 - (A) concerned in the provision of banking, insurance, investment or other financial services;
 - (B) concerned in the management of companies;
 - (BA) concerned in the administration of provident fund schemes registered under the Mandatory

Provident Fund Schemes Ordinance (Cap 485); (Added 4 of 1998 s. 14)

(C) concerned in the management of occupational retirement schemes within the meaning of the Occupational Retirement Schemes Ordinance (Cap 426); or

(D) who are shareholders in companies; or

(ii) the conduct of discharged or undischarged bankrupts;

(b) for maintaining or promoting the general stability or effective working of any of the systems which provide any of the services referred to in paragraph (a)(i)(A); or

(c) specified for the purposes of this subsection in a notice under subsection (4).

(4) For the purposes of subsection (3), the Chief Executive may, by notice in the Gazette, specify a function of a financial regulator. (Amended 34 of 1999 s. 3)

(5) It is hereby declared that-

(a) subsection (3) shall not operate to prejudice the generality of the operation of paragraphs (a), (b), (c), (d) and (f)(i) of subsection (1) in relation to a financial regulator;

(b) a notice under subsection (4) is subsidiary legislation.

(Enacted 1995)

Section:	58A	Protected product and relevant records under Interception of Communications and Surveillance Ordinance	20 of 2006	09/08/2006
----------	-----	--	------------	------------

(1) A personal data system is exempt from the provisions of this Ordinance to the extent that it is used by a data user for the collection, holding, processing or use of personal data which are, or are contained in, protected product or relevant records.

(2) Personal data which are, or are contained in, protected product or relevant records are exempt from the provisions of this Ordinance.

(3) In this section—

"device retrieval warrant" (器材取出手令) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (Cap 589);

"prescribed authorization" (訂明授權) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (Cap 589);

"protected product" (受保護成果) has the meaning assigned to it by section 2(1) of the Interception of Communications and Surveillance Ordinance (Cap 589);

"relevant records" (有關紀錄) means documents and records relating to—

(a) any application for the issue or renewal of any prescribed authorization or device retrieval warrant under the Interception of Communications and Surveillance Ordinance (Cap 589); or

(b) any prescribed authorization or device retrieval warrant issued or renewed under that Ordinance (including anything done pursuant to or in relation to such prescribed authorization or device retrieval warrant).

(Added 20 of 2006 s. 68)

Section:	59	Health		30/06/1997
----------	----	--------	--	------------

Personal data relating to the physical or mental health of the data subject are exempt from the provisions of either or both of-

(a) data protection principle 6 and section 18(1)(b);

(b) data protection principle 3,

in any case in which the application of those provisions to the data would be likely to cause serious harm to the physical or mental health of-

(i) the data subject; or

(ii) any other individual.

(Enacted 1995)

Section:	60	Legal professional privilege		30/06/1997
----------	----	------------------------------	--	------------

Personal data are exempt from the provisions of data protection principle 6 and section 18(1)(b) if the data consist of information in respect of which a claim to legal professional privilege could be maintained in law.

(Enacted 1995)

Section:	61	News		30/06/1997
----------	----	------	--	------------

- (1) Personal data held by a data user-
- (a) whose business, or part of whose business, consists of a news activity; and
 - (b) solely for the purpose of that activity (or any directly related activity),
- are exempt from the provisions of-
- (i) data protection principle 6 and sections 18(1)(b) and 38(i) unless and until the data are published or broadcast (wherever and by whatever means);
 - (ii) sections 36 and 38(b).
- (2) Personal data are exempt from the provisions of data protection principle 3 in any case in which-
- (a) the use of the data consists of disclosing the data to a data user referred to in subsection (1); and
 - (b) such disclosure is made by a person who has reasonable grounds to believe (and reasonably believes) that the publishing or broadcasting (wherever and by whatever means) of the data (and whether or not they are published or broadcast) is in the public interest.
- (3) In this section-
- "news activity" (新聞活動) means any journalistic activity and includes-
- (a) the-
 - (i) gathering of news;
 - (ii) preparation or compiling of articles or programmes concerning news; or
 - (iii) observations on news or current affairs,
 for the purpose of dissemination to the public; or
 - (b) the dissemination to the public of-
 - (i) any article or programme of or concerning news; or
 - (ii) observations on news or current affairs.

(Enacted 1995)

Section:	62	Statistics and research		30/06/1997
----------	----	-------------------------	--	------------

Personal data are exempt from the provisions of data protection principle 3 where-

- (a) the data are to be used for preparing statistics or carrying out research;
- (b) the data are not to be used for any other purpose; and
- (c) the resulting statistics or results of the research are not made available in a form which identifies the data subjects or any of them.

(Enacted 1995)

Section:	63	Exemption from section 18(1)(a)		30/06/1997
----------	----	---------------------------------	--	------------

Where a data access request relates to personal data which are or, if the data existed, would be exempt from section 18(1)(b) by virtue of section 57 or 58, then the data are also exempt from section 18(1)(a) if the interest protected by that exemption would be likely to be prejudiced by the disclosure of the existence or non-existence of those data.

(Enacted 1995)

Section:	63A	Human embryos, etc.	L.N. 164 of 2007	01/08/2007
----------	-----	---------------------	------------------	------------

(1) Personal data which consist of information showing that an identifiable individual was, or may have been, born in consequence of a reproductive technology procedure within the meaning of the Human Reproductive Technology Ordinance (Cap 561) are exempt from the provisions of data protection principle 6 and section 18(1)(b)

except so far as their disclosure under those provisions is made in accordance with section 33 of that Ordinance.

(2) Where a data access request relates to personal data which are or, if the data existed, would be exempt from section 18(1)(b) by virtue of subsection (1), then the data are also exempt from section 18(1)(a) if the interest protected by that exemption would be likely to be prejudiced by the disclosure of the existence or non-existence of the data.

(Added 47 of 2000 s. 48)

Section:	64	Offences		30/06/1997
----------	----	----------	--	------------

PART IX

OFFENCES AND COMPENSATION

- (1) A data user who, in any-
- (a) data user return submitted under section 14(4) to the Commissioner;
 - (b) notice under section 14(8) served on the Commissioner; or
 - (c) notice under section 15(3) or (4) submitted to or served on the Commissioner,
- knowingly or recklessly supplies any information-
- (i) which is false or misleading in a material particular; and
 - (ii) in purported compliance with that section,
- commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months.
- (2) A person who, in any data access request or data correction request, supplies any information-
- (a) which is false or misleading in a material particular; and
 - (b) which is so supplied for the purpose of having the data user concerned comply with the request,
- commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months.
- (3) A person who, in any notice under section 15(6) served on the Commissioner, supplies any information-
- (a) which is false or misleading in a material particular; and
 - (b) which is so supplied for the purpose of having the Commissioner comply with the request to which the notice relates,
- commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months.
- (4) A data user who, in any matching procedure request submitted to the Commissioner, supplies any information-
- (a) which is false or misleading in a material particular; and
 - (b) which is so supplied for the purpose of having the Commissioner consent to the matching procedure to which the request relates,
- commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months.
- (5) A data user (including a data user first-mentioned in section 32(2)) who contravenes any condition specified in a notice under section 30(2) or 32(1)(b)(i) commits an offence and is liable on conviction to a fine at level 3.
- (6) Any person who contravenes section 44(3) or 46(1) commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months.
- (7) Subject to subsection (8), any relevant data user who contravenes an enforcement notice served on the data user commits an offence and is liable on conviction to a fine at level 5 and to imprisonment for 2 years and, in the case of a continuing offence, to a daily penalty of \$1000.
- (8) It shall be a defence for a relevant data user charged with an offence under subsection (7) to show that the data user exercised all due diligence to comply with the enforcement notice concerned.
- (9) Any person who-
- (a) without lawful excuse, obstructs, hinders or resists the Commissioner or any other person in the performance of his functions or the exercise of his powers under Part VII;
 - (b) without lawful excuse, fails to comply with any lawful requirement of the Commissioner or any other person under that Part; or
 - (c) makes a statement which he knows to be false or does not believe to be true, or otherwise knowingly misleads the Commissioner or any other person in the performance of his functions or the exercise of his powers under that Part,
- commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months.
- (10) A data user who, without reasonable excuse, contravenes any requirement under this Ordinance (other than

a contravention of a data protection principle) for which no other penalty is specified in this section commits an offence and is liable on conviction to a fine at level 3.

(Enacted 1995)

Section:	65	Liability of employers and principals		30/06/1997
----------	----	---------------------------------------	--	------------

(1) Any act done or practice engaged in by a person in the course of his employment shall be treated for the purposes of this Ordinance as done or engaged in by his employer as well as by him, whether or not it was done or engaged in with the employer's knowledge or approval.

(2) Any act done or practice engaged in by a person as agent for another person with the authority (whether express or implied, and whether precedent or subsequent) of that other person shall be treated for the purposes of this Ordinance as done or engaged in by that other person as well as by him.

(3) In proceedings brought under this Ordinance against any person in respect of an act or practice alleged to have been done or engaged in, as the case may be, by an employee of his it shall be a defence for that person to prove that he took such steps as were practicable to prevent the employee from doing that act or engaging in that practice, or from doing or engaging in, in the course of his employment, acts or practices, as the case may be, of that description.

(4) For the avoidance of doubt, it is hereby declared that this section shall not apply for the purposes of any criminal proceedings.

(Enacted 1995)

Section:	66	Compensation		30/06/1997
----------	----	--------------	--	------------

(1) Subject to subsection (4), an individual who suffers damage by reason of a contravention-

- (a) of a requirement under this Ordinance;
- (b) by a data user; and
- (c) which relates, whether in whole or in part, to personal data of which that individual is the data subject,

shall be entitled to compensation from that data user for that damage.

(2) For the avoidance of doubt, it is hereby declared that damage referred to in subsection (1) may be or include injury to feelings.

(3) In any proceedings brought against any person by virtue of this section it shall be a defence to show that-

- (a) he had taken such care as in all the circumstances was reasonably required to avoid the contravention concerned; or
- (b) in any case where the contravention concerned occurred because the personal data concerned were inaccurate, the data accurately record data received or obtained by the data user concerned from the data subject or a third party.

(4) Where an individual suffers damage referred to in subsection (1) by reason of a contravention referred to in that subsection which occurred because the personal data concerned were inaccurate, then no compensation shall be payable under that subsection in respect of so much of that damage that has occurred at any time before the expiration of 1 year immediately following the day on which this section commences.

(Enacted 1995)

Section:	67	Power of Commissioner to specify forms		30/06/1997
----------	----	--	--	------------

PART X

MISCELLANEOUS

(1) Subject to subsection (2), the Commissioner may specify the form of any document required under this Ordinance to be in the specified form and the form of such other documents required for the purposes of this Ordinance as he thinks fit.

(2) The Commissioner's power under subsection (1) shall be subject to any express requirement under this Ordinance for a form, whether specified or otherwise, to comply with that requirement, but that requirement shall not restrict the exercise of that power in respect of that form to the extent that, in the opinion of the Commissioner, his exercise of that power in respect of that form does not contravene that requirement.

(3) The Commissioner's power under subsection (1) may be exercised in such a way as to-

- (a) include in the specified form of any document referred to in that subsection a statutory declaration-
 - (i) to be made by the person completing the form; and
 - (ii) as to whether the particulars contained in the form are true and correct to the best of that person's knowledge and belief;
 - (b) specify 2 or more forms of any document referred to in that subsection, whether as alternatives, or to provide for particular circumstances or particular cases, as the Commissioner thinks fit.
- (4) A form specified under this section shall be-
- (a) completed in accordance with such directions and instructions as are specified in the form;
 - (b) accompanied by such documents as are specified in the form; and
 - (c) if the completed form is required to be provided to-
 - (i) the Commissioner;
 - (ii) another person on behalf of the Commissioner; or
 - (iii) any other person,
 so provided in the manner, if any, specified in the form.

(Enacted 1995)

Section:	68	Service of notices		30/06/1997
----------	----	--------------------	--	------------

A notice (howsoever described) which is required to be served under this Ordinance, or which may be served under this Ordinance, on a person (howsoever described) shall, in the absence of evidence to the contrary, be deemed to be so served if-

- (a) in the case of an individual, it is-
 - (i) delivered to him;
 - (ii) left at his last known address for service, or at his last known place of residence or business, in Hong Kong;
 - (iii) sent by post to him at his last known address for service, or at his last known postal address, in Hong Kong; or
 - (iv) sent by telex, facsimile transmission or other similar method to him at his last known address for service, or at his last known postal address, or at his last known place of residence or business, in Hong Kong;
- (b) in the case of a company, it is-
 - (i) given to or served on an officer of the company;
 - (ii) left at the company's last known address for service, or at its last known place of business, in Hong Kong;
 - (iii) sent by post to the company at its last known address for service, or at its last known postal address, in Hong Kong; or
 - (iv) sent by telex, facsimile transmission or other similar method to the company at its last known address for service, or at its last known postal address, or at its last known place of business, in Hong Kong;
- (c) in the case of a partnership, it is-
 - (i) delivered, left or sent in accordance with paragraph (a) in respect of any partner who is an individual; or
 - (ii) given, served, left or sent in accordance with paragraph (b) in respect of any partner which is a company;
- (d) in the case of a person ("attorney") holding a power of attorney under which the attorney is authorized to accept service in respect of another person, it is-
 - (i) delivered, left or sent in accordance with paragraph (a) where the attorney is an individual;
 - (ii) given, served, left or sent in accordance with paragraph (b) where the attorney is a company;
 - (iii) delivered, left or sent in accordance with paragraph (a) in respect of any partner who is an individual where the attorney is a partnership; or
 - (iv) given, served, left or sent in accordance with paragraph (b) in respect of any partner which is a company where the attorney is a partnership.

(Enacted 1995)

Section:	69	Regulations - fees		30/06/1997
----------	----	--------------------	--	------------

(1) The Commissioner may make regulations to prescribe the fees to be paid in respect of any matter, service or facility in respect of which a prescribed fee is payable to the Commissioner under this Ordinance.

(2) The amount of any fee prescribed in regulations made under subsection (1) shall not be limited by reference to the amount of administrative or other costs incurred or likely to be incurred in relation to providing the matter, service or facility to which such fee relates, and different fees may be so prescribed for the same matter, service or facility in order to provide for particular circumstances or particular cases specified in the regulations.

(Enacted 1995)

Section:	70	Regulations - general	L.N. 130 of 2007	01/07/2007
----------	----	-----------------------	------------------	------------

Remarks:

For the saving and transitional provisions relating to the amendments made by the Resolution of the Legislative Council (L.N. 130 of 2007), see paragraph (12) of that Resolution.

(1) The Secretary for Constitutional and Mainland Affairs may make regulations for all or any of the following matters- (Amended L.N. 130 of 2007)

(a) the particulars to be entered in the log book of a data user, including particulars referred to in section 27(2)(a), (b) and (c);

(b) prescribing anything that is required or permitted to be prescribed under this Ordinance.

(2) Any regulations made under this section may-

(a) empower the Commissioner to grant exemptions from the regulations, either generally or in a particular case;

(b) make different provisions for different circumstances and provide for a particular case or class of case;

(c) be made so as to apply only in such circumstances as are prescribed by the regulations.

(3) Any regulations made under this section may prescribe offences in respect of contraventions of the regulations, and may provide for the imposition in respect of any such offence of a fine not exceeding level 3 and of imprisonment for a period not exceeding 2 years and, in the case of a continuing offence, to a daily penalty not exceeding \$1000.

(Enacted 1995)

Section:	71	Amendment of Schedules 2, 4 and 6	34 of 1999	01/07/1997
----------	----	-----------------------------------	------------	------------

Remarks:

Adaptation amendments retroactively made - see 34 of 1999 s. 3

The Chief Executive in Council may, by notice in the Gazette, amend Schedule 2, 4 or 6.

(Enacted 1995. Amended 34 of 1999 s. 3)

Section:	72	(Omitted as spent)		30/06/1997
----------	----	--------------------	--	------------

(Omitted as spent)

(Enacted 1995)

Section:	73	(Omitted as spent)		30/06/1997
----------	----	--------------------	--	------------

(Omitted as spent)

(Enacted 1995)

Schedule:	1	DATA PROTECTION PRINCIPLES		30/06/1997
-----------	---	----------------------------	--	------------

[sections 2(1) & (6)]

1. Principle 1-purpose and manner of collection of personal data

- (1) Personal data shall not be collected unless-
 - (a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
 - (b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and
 - (c) the data are adequate but not excessive in relation to that purpose.
 - (2) Personal data shall be collected by means which are-
 - (a) lawful; and
 - (b) fair in the circumstances of the case.
 - (3) Where the person from whom personal data are or are to be collected is the data subject, all practicable steps shall be taken to ensure that-
 - (a) he is explicitly or implicitly informed, on or before collecting the data, of-
 - (i) whether it is obligatory or voluntary for him to supply the data; and
 - (ii) where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and
 - (b) he is explicitly informed-
 - (i) on or before collecting the data, of-
 - (A) the purpose (in general or specific terms) for which the data are to be used; and
 - (B) the classes of persons to whom the data may be transferred; and
 - (ii) on or before first use of the data for the purpose for which they were collected, of-
 - (A) his rights to request access to and to request the correction of the data; and
 - (B) the name and address of the individual to whom any such request may be made,
- unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data are exempt from the provisions of data protection principle 6.

2. Principle 2-accuracy and duration of retention of personal data

- (1) All practicable steps shall be taken to ensure that-
 - (a) personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used;
 - (b) where there are reasonable grounds for believing that personal data are inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used-
 - (i) the data are not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise; or
 - (ii) the data are erased;
 - (c) where it is practicable in all the circumstances of the case to know that-
 - (i) personal data disclosed on or after the appointed day to a third party are materially inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used by the third party; and
 - (ii) that data were inaccurate at the time of such disclosure, that the third party-
 - (A) is informed that the data are inaccurate; and
 - (B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.
- (2) Personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used.

3. Principle 3-use of personal data

Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than-

- (a) the purpose for which the data were to be used at the time of the collection of the data; or
- (b) a purpose directly related to the purpose referred to in paragraph (a).

4. Principle 4-security of personal data

All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to-

- (a) the kind of data and the harm that could result if any of those things should occur;
- (b) the physical location where the data are stored;
- (c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;
- (d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data; and
- (e) any measures taken for ensuring the secure transmission of the data.

5. Principle 5-information to be generally available

All practicable steps shall be taken to ensure that a person can-

- (a) ascertain a data user's policies and practices in relation to personal data;
- (b) be informed of the kind of personal data held by a data user;
- (c) be informed of the main purposes for which personal data held by a data user are or are to be used.

6. Principle 6-access to personal data

A data subject shall be entitled to-

- (a) ascertain whether a data user holds personal data of which he is the data subject;
- (b) request access to personal data-
 - (i) within a reasonable time;
 - (ii) at a fee, if any, that is not excessive;
 - (iii) in a reasonable manner; and
 - (iv) in a form that is intelligible;
- (c) be given reasons if a request referred to in paragraph (b) is refused;
- (d) object to a refusal referred to in paragraph (c);
- (e) request the correction of personal data;
- (f) be given reasons if a request referred to in paragraph (e) is refused; and
- (g) object to a refusal referred to in paragraph (f).

(Enacted 1995)

Schedule:	2	FINANCES, ETC. OF COMMISSIONER	L.N. 130 of 2007	01/07/2007
-----------	---	--------------------------------	------------------	------------

Remarks:

For the saving and transitional provisions relating to the amendments made by the Resolution of the Legislative Council (L.N. 130 of 2007), see paragraph (12) of that Resolution.

[sections 5(7),
10(2)(c) & 71]

1. Resources of Commissioner

- (1) The resources of the Commissioner shall consist of-
 - (a) all money-
 - (i) paid by the Government to the Commissioner and appropriated for that purpose by the Legislative Council; and
 - (ii) otherwise provided to the Commissioner by the Government; and
 - (b) all other money and property, including gifts, donations, fees, rent, interest and accumulations of income received by the Commissioner.
- (2) The Secretary for Financial Services and the Treasury may give directions in writing of a general or specific character to the Commissioner in relation to the amount of money which may be expended by the Commissioner in any financial year and the Commissioner shall comply with those directions. (Amended L.N. 106 of 2002)
- (3) For the avoidance of doubt, it is hereby declared that any remuneration or other benefit payable to, and any expenses of-
 - (a) the Commissioner; or
 - (b) any person employed or engaged under section 9(1) of this Ordinance,shall be paid out of the resources of the Commissioner.

2. Borrowing powers

- (1) Subject to subsection (2), the Commissioner may borrow by way of overdraft such money as he may require for meeting his obligations or performing his functions under this Ordinance.
- (2) The Secretary for Constitutional and Mainland Affairs may, after consulting with the Secretary for Financial Services and the Treasury, give directions in writing of a general or specific character to the Commissioner in relation to the amount of money which may be borrowed under subsection (1) and the Commissioner shall comply with those directions.
- (3) The Commissioner may with the approval of the Secretary for Constitutional and Mainland Affairs given after the Secretary has consulted with the Secretary for Financial Services and the Treasury borrow, otherwise than by way of overdraft, such money as he may require for meeting his obligations or performing his functions under this Ordinance.
- (4) A person lending money to the Commissioner shall not be concerned to inquire whether the borrowing of the money is legal or regular or whether the money raised has been properly applied and shall not be prejudiced by any illegality or irregularity or by misapplication or non-application of the money.
(Amended L.N. 106 of 2002; L.N. 130 of 2007)

3. Investment of surplus funds

- (1) Subject to subsection (2), the Commissioner may invest money that is not immediately required to be expended.
- (2) The Commissioner shall not invest money pursuant to subsection (1) except in such forms of investment as the Secretary for Constitutional and Mainland Affairs, after consulting with the Secretary for Financial Services and the Treasury, approves. (Amended L.N. 106 of 2002; L.N. 130 of 2007)
- (3) Subsection (1) shall not be subject to section 10(1) of this Ordinance.

4. Accounts, audit and annual report of Commissioner

- (1) The Commissioner shall cause proper accounts to be kept of all his financial transactions.
- (2) The Commissioner shall, as soon as practicable after the expiry of a financial year, prepare a statement of the accounts of the Commissioner, which statement shall include an income and expenditure account and a balance sheet.
- (3) The Commissioner shall appoint an auditor who shall, as soon as practicable, audit the accounts required under subsection (1) and the statement of accounts required under subsection (2) and shall submit a report on the statement to the Commissioner.

(4) The Commissioner shall, as soon as practicable and in any case not later than 9 months after the expiry of a financial year (or such further period as the Chief Secretary for Administration allows), furnish-

(a) a report on the activities of the Commissioner during that year including a general survey of developments, during that year, in respect of matters falling within the scope of the Commissioner's functions;

(b) a copy of the statement of accounts required under subsection (2); and

(c) the auditor's report on the statement,

to the Chief Secretary for Administration who shall cause the same to be tabled in the Legislative Council. (Amended L.N. 362 of 1997)

(5) This section shall not be subject to section 10(1) of this Ordinance.

5. Director of Audit's examination

(1) The Director of Audit may, in respect of any financial year, conduct an examination into the economy, efficiency and effectiveness with which the Commissioner has expended his resources in performing his functions and exercising his powers.

(2) Subject to subsection (3), the Director of Audit shall have a right of access at all reasonable times to all such documents as he may reasonably require for conducting an examination under this section and shall be entitled to require from any person holding or being accountable for any such document such information and explanation as he considers reasonably necessary for that purpose.

(3) Subsection (2) applies only to documents in the custody and control of the Commissioner.

(4) The Director of Audit may report to the President of the Legislative Council the results of an examination conducted by him under this section.

(5) Subsection (1) shall not operate to entitle the Director of Audit to question the merits of the policy objectives of the Commissioner.

6. Exemption from taxation

(1) The Commissioner shall be exempt from taxation under the Inland Revenue Ordinance (Cap 112).

(2) For the avoidance of doubt, it is hereby declared that subsection (1) does not apply to or in relation to any remuneration, benefits or expenses referred to in section 1(3) paid out of the resources of the Commissioner to the Commissioner.

(Enacted 1995)

Schedule:	3	PRESCRIBED INFORMATION	30/06/1997
-----------	---	------------------------	------------

[section 14(10)]

1. The name and address of the data user.
2. A description of the kind of personal data in respect of which the data user is a data user.
3. A description of the purpose or purposes for which the personal data referred to in item 2 are or are to be collected, held, processed or used by the data user.
4. A description of any classes of persons to whom the data user discloses, intends to disclose or may wish to disclose the personal data referred to in item 2.
5. The names or a description of any places outside Hong Kong to which the data user transfers, intends to transfer or may wish to transfer, the personal data referred to in item 2.
6. The name and address of the individual to whom data access requests may be made to the data user.

(Enacted 1995)

Schedule:	4	PROVISIONS OF ORDINANCES UNDER WHICH MATCHING PROCEDURES ARE REQUIRED OR PERMITTED		30/06/1997
-----------	---	--	--	------------

[sections 30(1)(d) & 71]

(Enacted 1995)

Schedule:	5	PRESCRIBED MATTERS		30/06/1997
-----------	---	--------------------	--	------------

[section 32(4)]

1. Whether the carrying out of the matching procedure is in the public interest.
2. The kind of personal data to be the subject of the matching procedure.
3. The likely consequences to a data subject if the matching procedure were to result in any adverse action taken against the data subject.
4. The practices and procedures, if any, that will be followed to enable a data subject to make a data correction request-
 - (a) in respect any of the personal data produced or verified by the matching procedure;
 - (b) before any adverse action is taken against the data subject.
5. The practices and procedures, if any, that will be followed to ensure, so far as is practicable, the accuracy of any personal data produced or verified by the matching procedure.
6. Whether any such data subject is to be informed of the procedure before it is first carried out.
7. Whether there is any practicable alternative to the matching procedure.
8. The benefits to be derived from carrying out the matching procedure.

(Enacted 1995)

Schedule:	6			30/06/1997
-----------	---	--	--	------------

[sections 42(6), (7) & (11) & 71]

PART 1

WARRANT AUTHORIZING PRIVACY COMMISSIONER FOR PERSONAL DATA TO ENTER SPECIFIED PREMISES WITHOUT INFORMING RELEVANT DATA USER

To the Privacy Commissioner for Personal Data.

Having been satisfied by information upon oath/declaration* that there are reasonable grounds for believing that the purposes of an investigation under the Personal Data (Privacy) Ordinance (Cap 486) in relation to [name of relevant data user] may be substantially prejudiced if you were required to comply with section 42(3) of that Ordinance before exercising your power under section 42(2) of that Ordinance in respect of the premises at [address of premises occupied by the relevant data user/in which is situated the personal data system, or any part thereof, used by the relevant data user*]:

YOU ARE HEREBY AUTHORIZED, with such assistants as may be necessary, to exercise your power under section 42(2) of that Ordinance in respect of those premises without complying with section 42(3) of that Ordinance provided that such power is exercised before the expiration of 14 days after the date on which this warrant is issued.

Dated this day of 19

.....
(Signature) Magistrate

* Delete whichever is inapplicable.

PART 2

WARRANT AUTHORIZING PRIVACY COMMISSIONER FOR PERSONAL DATA TO ENTER SPECIFIED DOMESTIC PREMISES

To the Privacy Commissioner for Personal Data.

Having been satisfied by information upon oath/declaration* that there are reasonable grounds for believing that the purposes of the investigation into [name of relevant data user] may be substantially prejudiced if you are prevented by the operation of section 42(4) of the Personal Data (Privacy) Ordinance (Cap 486) from exercising your power under section 42(2) of that Ordinance in respect of the domestic premises at [address of domestic premises occupied by the relevant data user/in which is situated the personal data system, or any part thereof, used by the relevant data user*]:

YOU ARE HEREBY AUTHORIZED, with such assistants as may be necessary, to exercise that power in respect of those premises provided that such power is exercised before the expiration of 14 days after the date on which this warrant is issued.

Dated this day of 19

.....
(Signature) Magistrate

* Delete whichever is inapplicable.

(Enacted 1995)

A Short Guide to Data Protection in Hong Kong

Gabriela Kennedy (Partner)

1 March 2011

IPMT / Hong Kong



Agenda

- Basic Principles
- The Octopus case - what went wrong?
- Direct Marketing after the Octopus case
- Unsolicited Electronic Messages Ordinance
- Proposed reforms to the PDPO
- Asia-Pacific data protection round-up

Personal Data v. Privacy

- Right to be left alone?



- Personal Data (Privacy) Ordinance ("**PDPO**")

Personal Data v Privacy

- PDPO protects an individual's privacy to the extent it involves personal data

- General right to privacy:

- (i) Article 30 of the Basic Law:

The freedom and privacy of communication of Hong Kong residents shall be protected by law. No department or individual may, on any grounds, infringe upon the freedom and privacy of communication of residents except that the relevant authorities may inspect communication in accordance with legal procedures to meet the needs of public security or of investigation into criminal offences.

- (ii) Article 14 *Hong Kong Bill of Rights Ordinance*:

No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

15 years of data protection in Hong Kong

- PDPO enacted 3 August 1995 and in force 20 December 1996
- Underpinned by 6 data protection principles (DDPs) which govern:
 - data collection
 - accuracy and retention
 - use
 - security
 - availability of information
 - access and correction

Introduction to the Personal Data (Privacy) Ordinance (PDPO)

- Aims:
 - to protect the rights of individuals with respect to their personal data
 - to safeguard the free flow of personal data
- Applies to private sector and public sector

PDPO – Basic Concepts

- Data User
- Data Subject
- Personal Data
- No Notification / Registration Requirement
- No Extra-territorial Jurisdiction

Basic Concepts – Personal Data

- data must relate to living individuals (i.e. not companies)
- individual must be reasonably identifiable from data
- data must be documented and readily retrievable

(DPP1) – Purpose and Manner of Collection

- For lawful purposes
- Must not be excessive
- By fair means

Cathay Pacific Airways Ltd v Administrative Appeals Board HCAL
50/2008

- Data subjects must be notified of purposes of collection

Is A Photograph Personal Data?



Basic Concepts – Personal Data

- Is a photograph personal data?
Eastweek Publisher Ltd & Anor v Privacy Commissioner of Personal Data [2000] 1 HKC 692
- Is an email address personal data?
Shi Tao v Privacy Commissioner of Personal Data [2008] 1 HKC 287
- How about an IP address?

(DPP2) - Accuracy and Retention of Personal Data

- Personal data - accurate having regard to purpose
- Personal data not kept longer than necessary and required to fulfill purpose
- Corrections of data - transmitted to data users who supplied inaccurate data

(DPP3) - Use of Personal Data

- For the purposes for which data was collected and incidental purposes
- Use of data for any other purposes requires express consent of data subjects
Shi Tao v Privacy Commissioner for Personal Data [2008] 1 HKC 287
- No separate requirements for disclosure of data

(DPP3) – Use of Personal Data

- For purpose other than purpose of collection (or directly related purpose) if :
 - an exemption applies
 - prescribed consent is obtained

(DPP4) - Security of Personal Data

- Must take all reasonably practicable steps to protect personal data against unauthorised use and disclosure
- Policies
- Training
- Encryption?
- Outsourcing of data processing?
- Recent data leaks – changes to PDPO?

(DPP5) - Availability of Information

- Open and transparent data policies and practices
- Notice-boards
- Website statements

(DPP6) – Access to Personal Data

- Right to request a copy of personal data and/or correction of the data
- Who can request access?
Gotland Enterprises Ltd v Kwok Chi Yan HCMP 4550/2003
- Consequences of non-compliance
Jiang Enzhu v Lau Wai Hing Emily [1999] 3 HKC 8

Exemptions

- Applicable to DPPs 3 and 6 only:
 - Security, defence and international relations
 - Prevention and detection of crime
 - prevention, preclusion or remedying of unlawful or seriously improper conduct
 - Health
 - Legal professional privilege
 - News, statistics and research

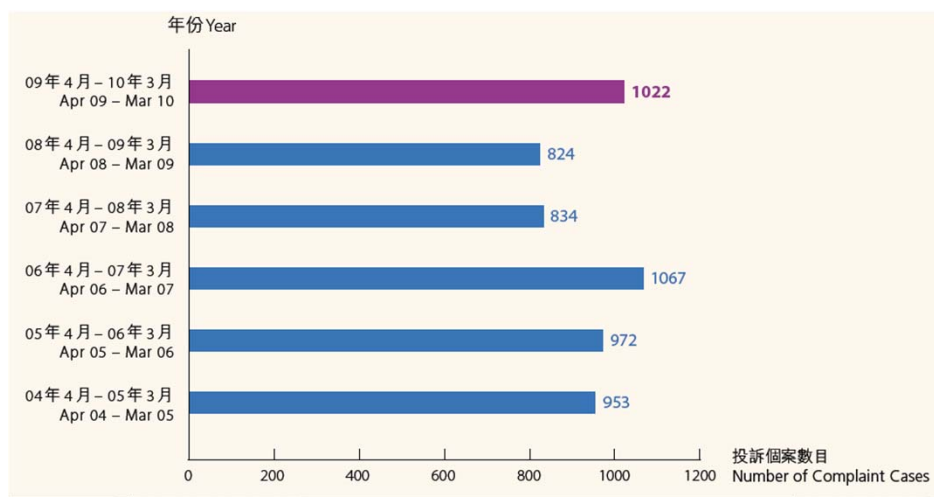
Transfer of Personal Data Outside Hong Kong

- S.33 PDPO – not yet in force
- Should comply with DPP3
- State intended transfer in PIC Statement
- Measures to be taken when processing is outsourced to companies outside Hong Kong

Non-compliance

- Investigations by Privacy Commissioner
- Enforcement notices
- Penalties / Offences
 - up to HK\$50,000 fine/ daily HK\$ 1,000 fine
 - up to 2 years jail
- Civil remedies
- Reputational damage

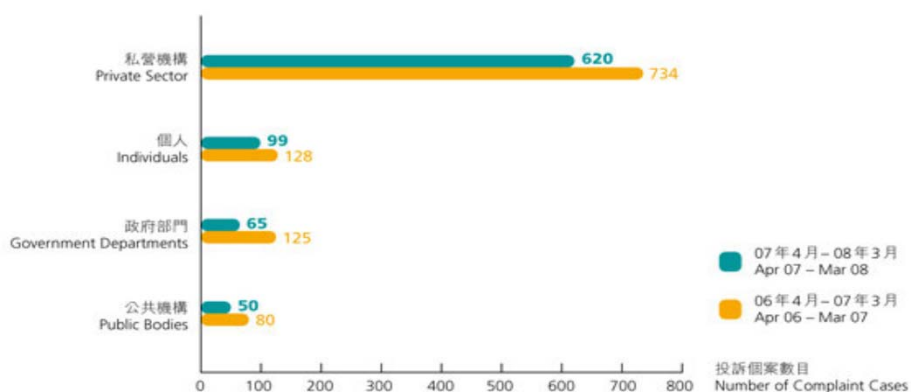
Complaint caseload: 2004 to 2010



www.hoganlovells.com

21

Parties complained against

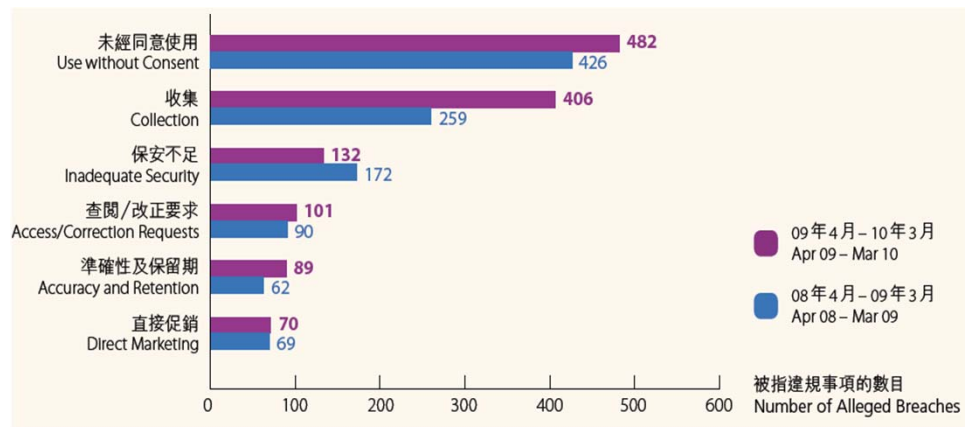


- 620 (74%) complaint cases were against private sector organizations.
- 115 (14%) complaint cases were against public sector organizations (i.e. government departments and other public bodies).
- 99 (12%) complaint cases were against individuals.

www.hoganlovells.com

22

Nature of Complaints



Summary of case statistics

Cases handled	2006	2007	2008
Enquiries	14 614	13 170	13 112
New applications for approval to carry out matching procedure	9	15	16
Complaints	1 208	1 074	946
Compliance checks	79	86	96
Enforcement notices issued	66*	14	7
Referrals for prosecution	8	9	5
Successful convictions	2	3	2

Codes of Practice

- Hong Kong Identity Card 1998
- Consumer Credit Data 1998 -2003
- Human Resource management 2000
- Workplace Surveillance 2001
- Protection of Customer Information for Fixed and Mobile Service Operators 2002
- Consequence of non-compliance with Codes of Practice

COP on ID Card Numbers and other personal identifiers

- When can an ID card number be requested? By whom?
- When can a copy of an ID card be taken? By whom?
- Examples for discussion:
 - lucky draws
 - supermarket loyalty programmes
 - access to buildings
 - mobile phone plans

Code of Practice on Human Resource Management

- Employment-related personal data issues:
 - "blind" advertisements
 - recruitment advertisements
 - retaining data of unsuccessful applicants, employees and former employees
 - non-disclosure of employee information to third parties
 - access to references; appraisal forms

Guidelines on Monitoring & Personal Data Privacy at Work

- 3As
 - **A**ssess the appropriateness of employee monitoring;
 - consider **A**lternatives to employee monitoring; and
 - recognise your **A**ccountability over employees' personal data privacy
- 3Cs
 - **C**larity in the employee monitoring policies;
 - **C**ommunicate the privacy policy to employees properly; and
 - **C**ontrol over the holding, processing and use of monitoring records

Data Protection DOs

Do:

- Implement and make available privacy collection statements which set out purposes of collection and access/correction right
- Implement and train employees on privacy policies and practices which reflect the requirements of the PDPO
- Encrypt all sensitive data held or transmitted online
- Provide "opt out" opportunities for any direct marketing
- Promote a "privacy aware" culture

Data Protection DON'Ts

Don't:

- Collect personal data from an individual without first providing them with a Privacy Collection Statement
- Collect more data than you actually need for the purposes of collection
- Collect HK ID Card numbers without giving individuals the option of providing an alternative personal identifier

The Octopus Rewards Program: What Went Wrong?

- Wide range of personal data collected
- Sale of personal data of almost 2 million card holders to 6 companies over nearly 8 years



The Investigation

- Formal investigation ordered by PC on 21 July 2010
- Witnesses summoned to give evidence at hearing
- Interim report issued on 30 July 2010 (unprecedented)



The Investigation



- DPP1- purpose and manner of collection: lawful? excessive?
- DPP3 - Use of personal data

(DPP1) – Purpose and Manner of Collection

- necessary
- not excessive
- for a lawful purpose directly related to the activity of the data user
- collected by lawful and fair means
- **Must inform the data subject of:**
 - the purpose of collection
 - the class of persons to whom the data may be transferred
 - the right to, and practicalities of, access to the data
 - whether it is obligatory to supply the data and, if so, the consequences of not doing so

DPP1- Was the Collection Excessive?

- My Info – required
- My Other Info - optional

八達通日日賞登記表格 Octopus Rewards Registration Form
 填寫此表格後，請將表格與您的八達通卡一併寄回或親臨八達通客戶服務中心。 (Please fill out this form and return it with your Octopus card to the Octopus Customer Service Centre.)

我的資料 My Information
 (請以正楷填寫，Please fill in with BLOCK LETTERS)
 (凡填必填項，Required Fields)

姓名 Name: [Redacted]
 ID #: [Redacted]
 護照號碼 Passport #: [Redacted]
 性別 Gender: [Redacted]
 E-mail: [Redacted]
 出生日期 DOB: [Redacted]
 聯絡電話 Contact #: [Redacted]
 地址 Address: [Redacted]

我的其他資料 My Other Information
 (以下資料將有助於我們為客戶提供最佳服務，請填妥此表格。 This will help us and our Partners to better identify selected offers that will be of interest and value to you.)

婚姻狀況 Marital Status: [Redacted]
 教育程度 Education Level: [Redacted]
 職業 Occupation: [Redacted]
 每月個人收入 Monthly Personal Income: [Redacted]
 每月家庭收入 Monthly Household Income: [Redacted]
 興趣 Interests: [Redacted]

我在此聲明，我提供的資料是真實、準確和完整的。 I hereby declare that the information I provide is true, accurate and complete.

申請人簽名 Signature of Applicant: [Redacted] 日期 Date: [Redacted]

DPP1 – Was the Collection Excessive?

- My Info: Octopus card no; English name; HKID No./ passport no/ birth cert no.; gender; month and year of birth; contact no; home address
- My Other Info – Chinese name; email; language; marital status; education level; occupation; monthly income; household income; interests
- Held: My Info – excessive collection (HKID/passport no/birth cert no; month and year of birth)
- Less intrusive data could have been collected/were sufficient

(DPP1)- Was the Information Fairly Collected?

- Reasonable expectation to have data communicated to Business Partners given nature of Rewards Programme
- No evidence of deception or coercion

DPP1(3) – Duty to Inform Data Subjects

- Take all reasonable and practicable steps to ensure data subject is explicitly informed on or before collection of purpose for which data is to be used and classes of persons to whom data may be transferred

DPP1(3)- Were Data Subjects Properly Informed?

- Registration Form
- Terms & Conditions (Clauses 6.3 and 6.4)
- Personal Information Collection Statement (PICS)
- Octopus didn't take all reasonable steps to inform its customers of the classes of transferees
 - classes of transferees identified in vague terms – in effect Octopus could transfer data to **any person** (within or outside Hong Kong)
 - PICS was printed in unreasonably small font

- Consent for disclosure of data to third parties "bundled" with acceptance of registration terms and conditions
- Inconvenient and time-consuming opt-out procedures
- Cross-reference to separate privacy terms and conditions

[illegible]

DPP1(3)- Duty to Inform Data Subjects

- DPP1(3) was contravened:
 - small print in PICS;
 - failure to define with any reasonable degree of certainty classes of transferees

Data Protection Principle 3 (DPP3) – Use of Personal Data

- Personal data should only be used for a purpose related to the purpose for which it was collected, unless the data subject expressly consents to another use



Octopus' Breach of (DPP3)

- Consent form gave broad consent to deal with personal information
- Personal data shared with business partners for monetary gain without prescribed consent
- Sale of personal data was not stated as a purpose of collection in PICS
- Sale of personal data was not the purpose of collection (or a directly related purpose)



Section 65(2) Acts of Agent

- Octopus Rewards – agent for Octopus Holding
- Octopus Holding – liable for the contraventions of Octopus Rewards

Results of Investigation

- Privacy Commissioner could not issue an enforcement notice to Octopus (Section 50 PDPO):
 - Octopus had ceased or suspended arrangements to sell personal data;
 - Octopus had already implemented various changes in its practice relating to data collection and use;
 - Repeat contraventions by Octopus – unlikely;
 - Undertaking provided by Octopus to Privacy Commissioner

Guidance Note on the Collection and Use of Personal Data in Direct Marketing – 18 October 2010

- Replaces the Fact Sheet on "Guidelines on Cold-Calling" and the Guidance Note on "Cross-Marketing Activities"
- Covers a number of issues included in proposed amendments and provides guidance on the PDPO as it currently stands
- Not part of PDPO

Guidance Note

- Collection of personal data for direct marketing should be related to the original purpose of data collection
- Personal data should not be excessively collected
- Collection of additional personal data for direct marketing should be voluntary (and the data subject should be informed of the voluntary nature of collection)

Guidance Note

- Personal data should not be collected using deceptive/misleading means
- The PICS should be effectively communicated to the data subject
- Data should be provided voluntarily
- No “bundled consent”
- The purpose of use of personal data and the classes of transferees should be clearly defined using specific terms.

Guidance Note

- Recommendations relating to :
 - use of personal data from public registers;
 - managing and maintaining opt-out lists and requests;
 - direct marketing activities conducted by agents, contractors and business partners
 - sale of personal data to third parties for direct marketing

Industry Specific Regulations - HKMA

- HKMA – 3 circulars between 12 August 2010 – 25 October 2010
- 25 October 2010 circular :
 - restates recommendations of Guidance Note
 - required reviews by end November 2010
 - transfer of personal data to unconnected third parties for marketing purposes suspended pending legal advice

Unsolicited Electronic Messages Ordinance (UEMO)

- Regulates "commercial electronic messages" with "Hong Kong link"
- Accurate sender information
- Unsubscribe facilities
- Language requirements (bi-lingual)
- Appropriate message recipients (Do-not-call Register/unsubscribed)
- Failure to comply with some provisions - offence (HK\$1 million fine + 5/10 years' jail)



Proposals for Reform - Chronology

28 August 2009

CMAB published Consultation Document
on Review of the PDPO

30 November 2009

End of Public consultation

October 2010

Further amendments proposed
as a result of Octopus case

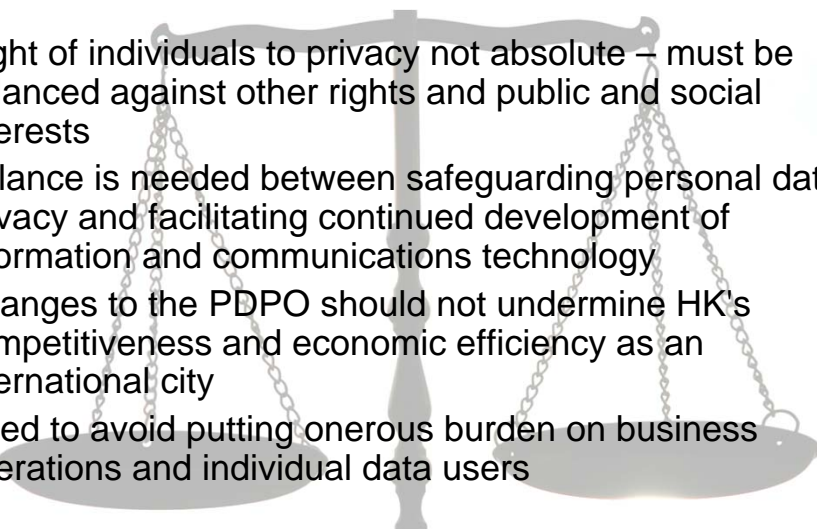
18 October 2010

Report on Public Consultation of
review of the PDPO

until 31 December 2010

37 proposals taken forward
and open to public comment

Guiding Principles

- 
- Right of individuals to privacy not absolute – must be balanced against other rights and public and social interests
 - Balance is needed between safeguarding personal data privacy and facilitating continued development of information and communications technology
 - Changes to the PDPO should not undermine HK's competitiveness and economic efficiency as an international city
 - Need to avoid putting onerous burden on business operations and individual data users

Proposals – 4 Major Areas

- Direct marketing and related matters
- Data security
- Powers of Privacy Commissioner
- Offences and sanctions

Direct Marketing – Requirements

Collection and Use	Sale of Personal Data
<ul style="list-style-type: none"> • PICS reasonably specific about: <ul style="list-style-type: none"> ➢ the intended direct marketing activities ➢ the classes of transferees ➢ the kinds of data to be transferred • PICS understandable and easily readable • Provide opt-out/opt-in facilities 	<ul style="list-style-type: none"> • Data user to inform the data subject <u>in writing</u> of: <ul style="list-style-type: none"> ➢ The person to whom their data may be sold ➢ the kinds of data to be sold • Such information should be understandable and easily readable • Provide opt-out/opt-in facilities

Direct Marketing – Offences

Collection and use	Sale of personal data
<p><u>Enforcement Notice</u> non-compliance with any of the Requirements</p>	<p><u>Enforcement Notice</u> non-compliance with any of the Requirements</p>
<p><u>Fine \$500,000 + 3 years imprisonment</u></p> <ul style="list-style-type: none"> • Fail to comply with Requirements + use of the data for direct marketing • Comply with Requirements but use data in way inconsistent with data subjects' consent or in a way other than as described in the PICS • Comply with Requirements but use personal data (or transfer to certain classes of transferees) when the subject data has indicated disagreement 	<p><u>Fines? Imprisonment?</u></p> <ul style="list-style-type: none"> • Fail to comply with Requirements + sale of personal data or sale against wish of data subject = offence (follow UEMO? HK\$1 million + 5 years' imprisonment?)

New Offence - Disclosure



- **New offence:** disclosure for profit or malicious purposes of data obtained without consent
- **What is "*malicious purpose*"?**
- 'with a view to gain for oneself or another, or with an intent to cause loss, which includes injury to feelings of another'?
- **Sanction:** same as for unauthorised sale of personal data

Data Security

Regulation of Data Processors & Sub-Contracting Activities

- Indirect v Direct regulatory model?
- Data users to use contractual or other means to ensure compliance with PDPO (Indirect)
- Contravention-> enforcement notice
- S. 65(2) PDPO – Data users liable for acts of agents
- Commissioner to increase publicity

Data Security

Personal Data Security Breach Notification

- Mandatory v voluntary breach notification system ?
 - Preference for voluntary notification system
 - supported by Guidance Note issued by the Commissioner:
 - *'Data Breach Handling and the Giving of Breach Notifications'* (21 June 2010)

Powers of Privacy Commissioner

- Provide legal assistance to an aggrieved data subject who intends to institute legal proceedings to seek compensation:
 - Give legal advice on the sufficiency of evidence
 - Arrange for legal representation for the applicant
 - Provide assistance where appropriate
- Power to issue EN even where breach is not likely to be repeated



New Offences and Sanctions

- Repeated Contravention of DPP on the same facts
 - **Current provision:** Enforcement notice (EN) followed by another EN
 - **Proposal:** Fine \$50,000 and imprisonment for 2 years
- Repeated non-compliance with Enforcement Notice
 - **Heavier penalties** are recommended: \$100,000 and imprisonment for 2 years (\$2,000 daily fine for continuing offences)



Miscellaneous Proposals

- Erasure of personal data
- Duty to prevent loss of personal data
- Transfer of data in Business Mergers and Acquisitions
- Use of Personal Data required or authorised by law or related legal proceedings
- Refusal to comply with data access request on ground of self-incrimination

Proposals Not Taken Forward

- Sensitive personal data
- Power for Commissioner to conduct criminal investigation and prosecution
- Power of the Commissioner to award compensation to aggrieved data subjects
- Making breach of DPP an offence
- Imposing monetary penalty on serious contravention of DPP
- Parents' right to access personal data of minors
- Maximum fee for handling data access requests



Asia Pacific Data Protection Round-up

Jurisdiction	Australia	Hong Kong	Japan	Malaysia*	PRC	Singapore	Vietnam	Taiwan*
Data protection legislation	Yes	Yes	Yes	Yes	No	No	No	Yes
Other relevant legislation/codes of practice	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Liability for acts of transferees/agents	Yes	Yes	Yes	?	No	No	No?	No
Registration requirements	No	No	No	Yes	Yes**	No	No	No (in most cases)
Mandatory breach notification requirements	No	No	No	No	N/A	N/A	N/A	No?
Restrictions on cross-border transfers	Yes	No	No	Yes	N/A	No	N/A	Yes
Civil remedies	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
Criminal sanctions	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes

* Data protection legislation has been passed but has not come into force yet.

** For certain industry sectors

People's Republic of China

- Draft Personal Information Protection Law was submitted to the State Council in 2005
- Amendment to Art. 253 Criminal Law - 2009
 - Unauthorised sale or provision of personal data is a criminal offence (only in case of serious breach by governmental officials / staff members of telecommunications, education and medical entities)
- Shanghai Pudong New District Court case (5 Aug 2010)
 - Illegal obtaining of personal data by *anyone* is a criminal offence under Art. 253
- Amendment to Consumer Protection Law (draft) 19 Oct 2010
 - Definition of **personal data**
 - **Penalties:** apologies / damages (actual loss and emotional distress)

Recent developments - Taiwan

- New Data Protection Act approved in April 2010 (not yet in force)
 - Applies to all individuals, organisations or enterprises that collect data (previously legislation only applied to a limited range of entities)
 - Expands scope of personal data (not just computer-processed data)
 - **Obligation to inform** data subject in case of data collection/use
 - Must be based on a **legitimate purpose** and with **prior consent** of the data subject
 - Collection of **sensitive personal data** (including genetic information) is forbidden unless legitimate reason
- Sanctions:
 - prohibition on collection and use of data
 - order deletion of data
 - seizure or destruction of unauthorised data
 - public announcement of violation
 - fines (companies and company representatives)
 - increased criminal penalties

Recent developments - Malaysia

- Personal Data Protection Act 2010 – passed in May 2010 (not yet in force)
 - Applies to any person who processes personal data in respect of *commercial transactions* by means of equipment
 - **7 Data Principles** (consent / notice and choice of the data subject / limited disclosure / security / retention / data integrity / access)
 - **Sensitive personal data** (including medical information) have more stringent provisions
 - Restrictions on **cross-border** transfer of data
 - **Criminal sanctions** (fines, imprisonment or both)

Recent Developments

- Japan
 - Guideline issued in 2009 to assist business operators handling personal data to understand the Personal Information Protection Act in the economic and industrial fields
 - privacy notice on business operator's website
 - notify the period that credit data will be stored
- Australia
 - Ongoing reform to include biometric data in the definition of sensitive personal data
 - mandatory breach notification?
 - legislative restrictions on cross-border transfer of data?

Questions?

www.hoganlovells.com

71

Gabriela Kennedy

Partner, IPMT

Hogan Lovells

11/F One Pacific Place

88 Queensway

Hong Kong

Tel: 2840 5084

Fax: 2537 1907

Email: gabriela.kennedy@hoganlovells.com

Blog: www.hldataprotection.com

www.hoganlovells.com

Hogan Lovells has offices in:

Abu Dhabi	Caracas	Hong Kong	Munich	Shanghai
Alicante	Colorado Springs	Houston	New York	Silicon Valley
Amsterdam	Denver	Jeddah*	Northern Virginia	Singapore
Baltimore	Dubai	London	Paris	Tokyo
Beijing	Dusseldorf	Los Angeles	Philadelphia	Ulaanbaatar*
Berlin	Frankfurt	Madrid	Prague	Warsaw
Boulder	Hamburg	Miami	Riyadh*	Washington DC
Brussels	Hanoi	Milan	Rome	Zagreb*
Budapest*	Ho Chi Minh City	Moscow	San Francisco	

*Hogan Lovells" or the "firm" refers to the international legal practice comprising Hogan Lovells International LLP, Hogan Lovells US LLP, Hogan Lovells Worldwide Group (a Swiss Verein), and their affiliated businesses, each of which is a separate legal entity. Hogan Lovells International LLP is a limited liability partnership registered in England and Wales with registered number OC323639. Registered office and principal place of business: Atlantic House, Holborn Viaduct, London EC1A 3PS. Hogan Lovells US LLP is a limited liability partnership registered in the District of Columbia.

The word "partner" is used to refer to a member of Hogan Lovells International LLP or a partner of Hogan Lovells US LLP, or an employee or consultant with equivalent standing and qualifications, and to a partner, member, employee or consultant in any of their affiliated businesses who has equivalent standing. Rankings and quotes from legal directories and other sources may refer to the former firms of Hogan & Hartson LLP and Lovells LLP. Where case studies are included, results achieved do not guarantee similar outcomes for other clients. New York State Notice: Attorney Advertising.

© Hogan Lovells 2010. All rights reserved.

* Associated offices

Have We Got News For You? : The Review of the Personal Data Privacy Legislation in Hong Kong

The Hong Kong Data Protection (Privacy) Ordinance (the "**Ordinance**") came into force in December 1996. Now, some 15 years later, the Ordinance is being overhauled in an effort to bring it in line with international privacy laws and standards, and to ensure its continued ability to provide adequate safeguards for the collection and use of personal data, given technological and other business developments over the last decade or so.

This article provides an overview of a number of the key proposals for reform against the background of reforms and developments of data protection regimes in other jurisdictions.

The main challenge when deciding and implementing proposals for reform is to be able to identify proposals that strike a balance between public and private interests. In the case of the proposed reform of the Ordinance, this involves balancing the need to protect the privacy rights of individuals (in respect of their personal data) with the need to avoid putting onerous burdens on data users, as such burdens may negatively impact the competitiveness and attractiveness of Hong Kong as an international city.

The overhaul of the Ordinance was first proposed in August 2009 when the Constitutional and Mainland Affairs Bureau ("**CMAB**") put forward for public comment the Consultation Document on the Review of the Personal Data (Privacy) Ordinance (the "**Consultation Document**").

A year later in 2010, as a result of a highly publicised incident involving the sale of personal data by a subsidiary of the operator of stored value cards in Hong Kong, Octopus Holdings Limited ("**Octopus**") a number of additional reforms were proposed to address concerns regarding the transfer of personal data for direct marketing purposes.

The "Report on Public Consultation on Review of the Personal Data (Privacy) Ordinance" (the "**Report**") released by the CMBA on 18 October 2010, encompasses the most recent round of proposed reforms of the Ordinance. The Report contains 37 proposals which fall into four main areas (i.e. direct marketing, data security, powers of the Privacy Commissioner of Personal Data ("**the Commissioner**") and new offences and sanctions), as well as a number of other miscellaneous proposals. Although the Report may seem ambitious, it is to be noted that 18 amendments proposed in the Consultation Document back in 2009 were not taken forward and were not incorporated in the Report.

When the Consultation Document was published, the then Commissioner, Mr. Roderic Woo presented to the CMAB the results of his own review of the Ordinance. The Consultation Document contained some but by no means all of the issues captured in the Commissioner's

review. The Commissioner subsequently released his submissions in response to the Consultation Document, responding to the various proposals and noting that the Government's proposals were "more moderate and conservative" than those made by him.

A number of the main proposals for reform are outlined below.

Powers of the Privacy Commissioner

The main criticism of the Ordinance over the years has been that it has no teeth. Under the current provisions of the Ordinance, the Commissioner is only empowered to conduct investigations and issue enforcement notices in the event of a breach of a data protection principle. During his tenure as Commissioner, Mr. Roderick Woo, made the point on a number of occasions that the powers of the Commissioner had to be strengthened, and advocated powers that would allow the Commissioner to carry out criminal investigation and prosecution (which he viewed as directly related to his ability to enforce the Ordinance), as well as to provide legal assistance to data subjects. The current Commissioner, Mr. Allan Chiang, has also expressed concern that his powers are not adequate.

The Consultation Document contained a number of proposals designed to increase the powers of the Commissioner, which were ultimately not taken forward in the Report. These proposals, including introducing criminal investigation and prosecution powers, as well as the power to award compensation to aggrieved data subjects, were the subject of much public debate, with concerns being expressed that such powers should be vested in the police and the Department of Justice as it would be undesirable to concentrate enforcement and punitive functions in a single authority.

Aggrieved data subjects are entitled under the Ordinance to commence civil proceedings and seek damages as a result of a breach of a data protection principle. However, given the cost of such proceedings the provision has rarely been invoked. While there are concerns that in a common law legal system, the power to award compensation should be left to the Courts, in Australia, the Privacy Commissioner is entitled to award damages to data subjects based on their actual loss or damage. In fact, the powers of the Australian Privacy Commissioner go one step further and empower him to act as conciliator between complainants and respondents in data privacy disputes.

Although in practice under the current provisions of the Ordinance the Commissioner does engage in a mediatory role as a first step, he is advocating that a more formalised approach for mediation similar to the one in Australia, should be implemented in Hong Kong. This would provide an additional, quicker and more cost effective remedy to aggrieved data subjects and would likely result in data subjects being more willing to take action in respect of breaches of their

personal data privacy. While this is clearly advantageous for data subjects, the practical implications would need to be considered, in particular whether the Commissioner's office has the resources to handle the potential influx of mediations that may result from the introduction of such powers.

The Report does however propose a number of reforms which are designed to enhance the Commissioner's enforcement powers. One of the primary proposals relates to empowering the Commissioner to issue enforcement notices even when a breach of the Ordinance is not likely to be repeated. Under the current provisions, the Commissioner may only issue an enforcement notice if the contravention is ongoing, or where such contravention is likely to be repeated. This restriction came under public scrutiny as a result of the Octopus incident, where despite the Commissioner's finding that Octopus had breached the Ordinance, the Commissioner was unable to issue an enforcement notice as a reoccurrence of the contravention was unlikely given that the sale of personal data had ceased and Octopus had undertaken to take steps to ensure compliance with the Ordinance in the future.

The Commissioner's inability to issue an enforcement notice in the Octopus case, brought to the fore the question of the effectiveness of the Ordinance. The incident highlighted the gap between the Commissioner's enforcement powers under the Ordinance and public expectations relating to the punishment of offenders, a fact which was recognised by the Commissioner and which has clearly influenced a number of proposals contained in the Report.

The new proposed measure will empower the Commissioner to issue a notice even when the contravention has ceased, provided that it has caused or is likely to cause damage or distress to data subjects.

New offences and sanctions

In addition to strengthening the powers of the Commissioner, in an attempt to give the Ordinance more teeth, the Report also proposes a number of new offences and sanctions, including the introduction of offences for repeated contraventions of a Data Protection Principle ("**DPP**"). The Ordinance is underpinned by six DPPs. If a data user does not comply with a DPP, the Commissioner may under certain circumstances serve an enforcement notice specifying remedial steps to be taken by the data user. If the data user complies with the enforcement notice, but subsequently repeats the contravening act on the same facts, the current provisions of the Ordinance only enable the Commissioner to issue a fresh enforcement notice. As a result, data users could intentionally breach a DPP after having complied with an enforcement notice on the same facts, with very little fear of increased repercussions. In order to plug this loophole, the introduction of a new offence has been proposed, where a repeated contravention of a DPP occurs. Such an offence would attract a fine of HK\$ 50,000 and imprisonment for two years.

Non-compliance with an enforcement notice attracts a HK\$ 50,000 fine and two years' imprisonment, with a daily fine of HK\$ 1,000 for continuing offences but there is no sanction for repeated non-compliance with an enforcement notice. To deal with this it is proposed that heavier penalties are introduced for repeated non-compliance with enforcement notices, namely a fine of up to HK\$ 100,000 and imprisonment for two years, and a daily fine of HK\$ 2,000 for continuing offences.

A number of additional new offences have been proposed relating to the use and sale of personal data in direct marketing, and disclosure of personal data for malicious purposes, which are discussed in more detail below.

Direct marketing

Given the furore caused by the revelation that the personal data of 2 million customers had been sold by Octopus for direct marketing purposes, there is no surprise that a number of amendments have been proposed to deal with this specific type of transfer of personal data.

Use/transfer of data for direct marketing

Section 34 of the Ordinance currently provides that data users intending to use personal data for direct marketing purposes, must provide an opt-out to data subjects at the time of the first use of such data for direct marketing. The Report proposes amending section 34 by imposing a number of mandatory requirements where personal data is to be transferred for direct marketing purposes (the "**Requirements**"), including the following:

- (a) the presentation of a Personal Information Collection Statement ("**PICS**"), which clearly sets out direct marketing activities proposed, the classes of transferees and the kinds of data to be transferred;
- (b) the presentation of the PICS in a form that makes it understandable and easily readable (in other words the PICS should not be written in unreasonably small font, or lead data subjects to give their consent without noticing or understanding the content of the statement); and
- (c) an opt-out facility which shall be communicated to data subjects on or before the collection of the personal data. This is designed to prevent cases of bundled consent where data subjects have no choice but to consent to their personal data being used for direct marketing, if they order wish to see though the process/application for which the personal information is being collected.

Like other provisions in the Ordinance, a breach of section 34 constitutes an offence, but it only attracts a paltry fine of HK\$ 10,000. Such a small penalty clearly does not have a sufficient deterrent effect, particularly to large companies for which such a fine is a mere trifle. The Report proposes that this penalty be increased to a fine of HK\$ 500,000 and imprisonment for three years.

A number of other sanctions in relation to direct marketing are proposed as follows:

- (a) if the data user does not comply with any of the Requirements, the Commissioner will have the power to issue an enforcement notice to the data user;
- (b) fines of up to HK\$ 500,000 and 3 years of imprisonment may be imposed, if data users:
 - (i) fail to comply with any of the Requirements *and* use the data for direct marketing;
 - (ii) comply with the Requirements but use the data for direct marketing after a data subject has opted-out of their data being used for such purposes; or
 - (iii) comply with the Requirements but use the data in a way inconsistent with the PICS.

Sale of data for direct marketing

The current Ordinance does not contain provisions specifically relating to the sale of personal data for direct marketing, nor do the current provisions prohibit such sale. The Report contains proposals for the regulation of the sale of such data. It is proposed that prior to selling personal data, data users must inform data subjects in writing (via a PICS) of the persons to whom their data may be sold and the kinds of data that may be sold. The information must be understandable and reasonably readable, and opt-out/opt-in facilities must be provided. The Commissioner will have the power to issue an enforcement notice in the event that these requirements are not complied with.

The Report also proposes the creation of a new offence where a data user sells personal data without complying with the above requirements, or does so against the wish of the data subject. A penalty has not yet been determined for this offence, however, the CMAB has made reference to the provisions of the Unsolicited Electronic Message Ordinance, where fines of up to HK\$ 100,000 may be incurred for failing to comply with unsubscribe requests, or in the case of intentional contraventions, fines of up to HK\$ 1 million and imprisonment for five years.

When preparing The Report, the administration looked at data protection legislation in other jurisdictions, such as the United Kingdom, Australia and New Zealand. Interestingly, none of these prohibit or criminalise the sale of personal data. If the new sanctions proposed are adopted, Hong Kong will be at the forefront of regulation in this area.

Disclosure of data for malicious purposes or profits

The Report introduces a new offence in case of disclosure for profit or malicious purpose of data obtained from a data user without the data user's consent. An example of where this offence may apply is where an employee takes personal data handled in the course of his/her employment and sells it to a direct marketing company. The new provision makes that employee, rather than the employer, liable for the unauthorised disclosure of the personal data.

The penalty for this new offence is yet to be determined, but the CMAB has commented that it may be appropriate to impose similar penalties to those proposed in the relation to the sale of personal data.

This offence is reminiscent of section 55 of the UK *Data Protection Act* which prohibits the deliberate or reckless obtaining or disclosure of personal data without the consent of the data controller, as well as the subsequent sale or offer to sell such data. The UK legislation contains various defences, including where a person had a reasonable belief that he/she had the right to obtain the data or that the data controller would have consented to the obtaining of the information. The Report proposes that that similar defences be implemented in Hong Kong.

There are a number of important differences however between the UK provisions and the Hong Kong proposals. The Hong Kong proposals do not incorporate the UK requirement that the disclosure be made "knowingly or recklessly", but rather include a much narrower requirement that the act be carried out with a "malicious purpose" or for profit. While an exact definition of "malicious purpose" has not been suggested, the Report proposes that it includes data obtained *"with a view to gain for oneself or another, or with an intent to cause loss, which includes injury to feelings, to another"*.

The proposal is undoubtedly a positive step towards regulating the intentional mishandling of personal data. However, the narrow requirements of the Hong Kong proposals may result in serious wilful breaches not being caught by this offence. A broader offence (similar to that in place in the UK), would be more effective in capturing all forms of wilful mishandling of personal data.

Data security

Given the increased trend to employ third party processors to handle and process data, the issue of the security of data has become more and more important.

Regulation of data processors

Under section 65(2) of the Ordinance, data users are liable for the acts of their agents. However, many consider that this is not an adequate safeguard, especially given the potential consequences resulting from the mishandling of data by a data processor. While it has been acknowledged that increased regulation of data processors is required, there has been much debate as to whether data processors should be directly regulated, or whether they should be regulated indirectly through the data user (i.e. by contractual or other means). No consensus was reached on this point during the consultation period for the Consultation Document, with the public equally supporting both models.

The Ordinance does not contain a definition for "data processor" and data processors are expressly excluded from the definition of "data user" under the Ordinance. By contrast, the UK *Data Protection Act* and the *European Union Directive 95/46/EC*, include definitions of "data processors". The CMAB expressed concern that direct regulation of data processors may prejudice Hong Kong's attractiveness as a place for data processing and encourage businesses to outsource the processing of data to other countries. The Report proposes an indirect regulatory approach, encouraging data users to use contractual and other means to ensure that data processors comply with the requirements of the Ordinance, and requiring the Commissioner to conduct a public education campaign and provide guidelines and guidance on the relationship between data users and data processors.

Given the increased prevalence of external data processing and the potential harm that may result to data subjects if their personal data is mishandled by data processors, it may not be adequate to rely on the data user alone to regulate the acts of data processors. While under an indirect regulatory approach the data processor may be subject to civil penalties if they mishandle personal data, the Commissioner will not be able to regulate or investigate them directly, and data users will be solely liable for any infringing acts of the processor under section 65(2) of the Ordinance. Further, data subjects would not be able to bring a claim against data processors directly (in addition to any claim they may have against data users).

A number of submissions cited in the Report support the indirect regulatory approach and make reference to the difficulties associated with formulating provisions that would apply to the many different categories of data processors. This then raises the question of whether the direct regulatory model should be abandoned simply because it is difficult to define its scope and application.

Data breach notifications

A proposal linked to the data security proposals is the notification requirement for data breaches. This proposal was prompted by a series of high profile data leakages in Hong Kong over the last few years. While it was generally agreed that a breach notification system should be implemented, much debate in relation to this proposal centered on whether the notification system should be mandatory or voluntary. The Report proposes a voluntary system, on the basis that given that the concept of breach notification is relatively new to Hong Kong, a voluntary system would be a good transitional measure. The Consultation Document (which was echoed by the Report) proposed that this voluntary notification system should be complemented by guidance from the Privacy Commissioner in relation to the action required in the event of a security breach. In response to this, and in anticipation of the reforms, the Commissioner published a Guidance Note on "Data Breach Handling and the Giving of Breach Notifications in June 2010.

However, concerns were raised during the public consultation that a voluntary system will not provide adequate incentive for data users to report breaches. Mandatory notification systems have been adopted in a number of jurisdictions already. The United States has implemented a mandatory system and a bill to this effect has been introduced in Canada. In addition, the *European Union Directive 2002/58* contains breach reporting requirements for telecommunications providers and internet service providers, and consideration is being given extending these requirements to other sectors. A number of EU member states, namely Austria and Germany, have recently introduced reporting requirements in their national legislation. Other countries such as Australia and Ireland are currently considering proposals to implement such systems.

The Commissioner's view appears to be that given the world trend towards mandatory notification, the current proposals do not go far enough. In order for a breach notification system to be effective, it must be mandatory. There was much support for a mandatory approach during the consultation period, and some arguments were made that would not be premature to implement a mandatory system, given that a Guidance Note was issued last year setting out the requirements for data breach notifications.

While a mandatory breach notification system would undoubtedly impose a burden on data users, this must be balanced against the need to safeguard the safety and security of personal data and the potential detriment that may be suffered by data subjects in the event of unreported data breaches. These consequences could be particularly serious in breaches involving sensitive personal data, such as patient records held by hospitals. While the mandatory reporting scheme received much support during the consultation period, the prevailing public opinion appears to be that Hong Kong is not ready for a mandatory breach notification system. However, it should be noted that while a voluntary system could be generally implemented, exceptions could be introduced for certain industries or sectors where breaches of data security could have particularly serious consequences for data subjects. This is consistent with the approach in the EU, where the breach reporting requirements are being considered on a sector by sector basis.

Cross-jurisdictional transfer of personal data

One point of discussion throughout the review and consultation process was the fact that section 33 of the Ordinance was excluded from consideration. Section 33 restricts, subject to certain exceptions, the transfer of personal data from Hong Kong to any jurisdiction that lacks an adequate data protection regime, and is the only section of the Ordinance that has not yet been brought into force, despite being on the statute books for the last 15 years. With the increasing internationalisation of business, and the ability to disseminate information across the world instantaneously through the Internet, the protection and regulation of cross jurisdictional personal data transfers has come under increasing scrutiny.

As long as section 33 is not in force there is effectively no restriction on the transfer of personal data to jurisdictions without a data protection regime (most significantly, mainland China). This in turn means that parties wishing to protect personal data transfers to such jurisdictions must rely on (and, in cases of breach, take steps to enforce) contractual terms restricting the use of the transferred data. Unauthorised use of personal data in this way is a matter of contract, rather than statutory law.

The review of the ordinance was long overdue, whether the proposals tabled go far enough is another matter.

Gabriela Kennedy (Partner) (gabriela.kennedy@hoganlovells.com), Heidi Gleeson (Registered Foreign Lawyer) Hogan Lovells, Hong Kong

MAJOR CREDIT AGENCY PASSES TEST OF PRIVACY COMMISSIONER INSPECTION

The Privacy Commissioner for Personal Data (the "**Commissioner**") has recently exercised his rights under Section 36 of the *Personal Data (Privacy) Ordinance* (the "**Ordinance**"), and conducted an inspection of the data system of TransUnion Limited ("**TransUnion**"), Hong Kong's major credit reference agency ("**CRA**"). While the inspection did not reveal any major data breaches or issues, the Commissioner has reported deficiencies in TransUnion's personal data system and made a number of recommendations for improvement.

TransUnion holds the credit records of approximately 4.3 million consumers in Hong Kong and is the main source of consumer credit data for credit providers. Given the large amount of data held by TransUnion and the risk of loss and damages to consumers in the event that this sensitive personal data were misused, the Commissioner considered that an inspection was warranted.

The major objective of the inspection was to review the data processing cycle of TransUnion to ascertain whether it complies with the data protection principles under the Ordinance (the "DPPs") and with the Code of Practice on Consumer Credit Data (the '**Code**'), which was issued to provide guidance to CRAs when collecting, storing and processing personal data.

The Inspection Report

On 15 March 2011, the Commissioner issued his inspection report (the "**Report**"). Whilst the Report noted that TransUnion had in place comprehensive and detailed policies regarding the handling of consumer credit data it also noted areas where there was room for improvement and made twenty recommendations for TransUnion to enhance its personal data system.

The investigation report and its recommendations provide useful guidance for businesses as regards compliance with the data protection requirements under the Ordinance and the Code. We examine below the main recommendations made by the Commissioner.

Purpose and manner of collection of personal data

DPP1 requires that personal data are only collected for a specific purpose and not excessively in relation to that purpose. The Code identifies eight kinds of personal data that may be collected by a CRA, including consumer credit data and public records relating to any debt recovery action. A CRA that collects personal data outside of the eight categories specified in the Code is presumed to have breached DPP1.

The investigation revealed that TransUnion was collecting excessive information about consumers including winding-up court records about company winding-up procedures and personal injury records. The Commission recommended that TransUnion ceases to collect such

records (and should destroy any records of such data already collected), as they did not fall within the categories of permitted information under the Code.

Accuracy and retention of personal data

DPP2 requires data users to take reasonable steps in order to ensure the accuracy of personal data collected. Accuracy of credit consumer data is particularly significant given that consumer creditworthiness is evaluated based on such data.

Under the Code, the obligation to provide accurate data falls on the credit providers that supply the personal data to TransUnion ("**Subscribers**"). While no such obligation is placed on TransUnion under the Code, the Commissioner indicated that it was good practice for TransUnion to double-check the consumer credit data provided by Subscribers in order to detect inaccuracies.

DPP2 also requires that personal data is only kept so long as necessary for the fulfilment of the purpose for which it was collected. The Commissioner recommended that TransUnion specify the retention period on its request forms and supporting documents as well as in the relevant terms and conditions, and that personal data collection forms should not be kept for more than one year, after which time it should be completely destroyed.

Data security

The security obligations under the Ordinance impose a duty on data users to take all reasonably practicable steps to ensure that the personal data they hold is protected against unauthorised or accidental access, processing or erasure. Further, the Code requires CRAs to deploy a number of security measures to safeguard the personal data they hold, including entering into written agreements with the Subscribers by which the latter agree to abide by the DPPs, recording any data breach incidents, and training staff.

The Commissioner urged TransUnion to enhance its security standards by carrying out regular risk assessment and IT security audits. The Commissioner emphasised the importance of training and encouraged TransUnion to conduct regular compliance sessions for its staff.

The investigation revealed the following:

- (i) TransUnion outsources the storage of backup tapes containing consumer credit data to a third party (the "**Security Company**");
- (ii) TransUnion's security procedures when sending data to off-site data rooms leave a lot to be desired (e.g. transportation of the tapes by a security guard by public transport);
- (iii) the Security Company had a contractual right to access TransUnion's the data but without the backup of contractual provisions relating to data protection compliance or confidentiality;

- (iv) there were loopholes and gaps in the security of electronic storage devices used by TransUnion.;
- (v) TransUnion had commissioned a third party (the "**Data Disposal Company**") to dispose of its electronic storage media;
- (vi) there was no comprehensive written agreement between the Data Disposal Company and TransUnion,

The Commissioner was dissatisfied with the way TransUnion was dealing with the Security Company and the Report reinforced the fact that under the Ordinance, it is the data user (i.e. TransUnion) who is liable for the acts of its agent (i.e. the Security Company). The Commissioner encouraged TransUnion: (i) to take appropriate measures to prevent other incidents in the future; (ii) to introduce a duty of confidentiality in its existing agreement with the Security Company and also recommended that TransUnion enter into a written agreement with the Data Disposal Company, containing provision relating to security and confidentiality of data.

Public consultation into the sharing of positive mortgage data

A public consultation was recently carried out regarding proposals made by the financial services industry to widen the scope of the current data sharing regime in Hong Kong to include the sharing of positive mortgage data in certain circumstances. If implemented, the proposals would result in CRAs collecting and storing an increased amount of sensitive personal data, and it would become even more important for TransUnion to ensure that it had a secure data system.

The consultation period ended in January this year and the results of the consultation are yet to be announced. Further updates will be forthcoming when the results of the public consultation are published.

Gabriela Kennedy (Partner) gabriela.kennedy@hoganlovells.com, Heidi Gleeson (Registered Foreign Lawyer) and Alya Bloum (Intern), Hogan Lovells, Hong Kong

People's Republic of China (PRC)

DRAFT PRC GUIDELINES ON PERSONAL DATA PROTECTION

While personal data privacy law has been developing in many jurisdictions with the increasing prevalence of internet usage, the People's Republic of China ("**PRC**") has not yet enacted comprehensive laws or regulations governing the collection, use and transfer of personal data. However, this may change soon, as indicated by the recent issuance of the draft *Information*

Security Technology -- Guide of Personal Information Protection (the "**Guidelines**", issued jointly by the General Administration of Quality Supervision Inspection and Quarantine and the Standardization Administration of the PRC on 30 January 2011). The draft Guidelines were developed in consultation with the Ministry of Industry and Information Technology, the government agency charged with regulating the telecoms and internet industries, and would create broadly applicable rules and principles for handling and transferring personal information. Although the draft Guidelines could be revised before implementation and have not yet been enacted, upon entering into force they could significantly impact business practices relating to storage, processing and transfer of information.

CURRENTLY APPLICABLE LAWS AND REGULATIONS

In the absence of comprehensive PRC laws or regulations on personal information protection, businesses have had little guidance on the types of activities which are permissible. Generally, the *Constitution of the People's Republic of China* ("**PRC Constitution**") sets forth rights which have been interpreted by academics as establishing an individual right to privacy. Article 40 of the PRC Constitution provides that a citizen's freedom of communications and privacy of communications are protected by law. Article 38 of the PRC Constitution sets forth a general right of citizens to be free from infringements on their dignity, and protects citizens from defamation, false accusations and insults. These articles have been interpreted as the foundation for a general right to privacy which is briefly mentioned in various PRC laws and regulations. For example, the seventh amendment to the PRC *Criminal Law* (effective 28 February 2009) added the criminal offenses of illegally providing and illegally using personal information of PRC citizens. Both individuals and legal entities may be found guilty of the offenses: legal entities may liable for fines, and responsible individual management personnel may be subject to fines and imprisonment and/or probation for up to 3 years. Despite potentially harsh penalties, little regulatory guidance has been given on the types of behavior which are illegal when collecting and processing personal information. Although a draft *Personal Information Protection Law* ("**Draft Privacy Law**") was published in late 2006, it remains under review and has not been enacted. The draft Guidelines would partially fill this void, but in many ways could present compliance challenges for businesses.

KEY FEATURES OF THE DRAFT GUIDELINES

The draft Guidelines could have widespread effects on the way multinational corporations operate in China. By broadly defining "personal information", granting data subjects broad rights relating to personal information and tightly limiting the ability of data processors to transfer information, compliance with the draft Guidelines could prove costly and time-consuming.

Broad scope

The draft Guidelines would apply to all use of computer systems in processing personal information, including the collection, processing, transfer, use, prevention of access and deletion

of personal information. Personal information is also broadly defined as any information which independently or together with other information enables identification of the data subject. The definition of personal information is broad enough to conceivably cover any type of information relating to a person.

General principles

The draft Guidelines provide general principles for processing personal information. The purpose and use of collecting personal information should be clear and reasonable. Data processors should notify data subjects in plain language of: (1) the purpose of collecting the personal information and the scope of use, (2) the period of storing the information, (3) information protection policies in place to safeguard the information, (4) the rights of the data subject, (5) the individual responsible for data processing, and (6) other relevant information. Personal information should not be collected or processed without the informed consent of the data subject.

Rights of data subjects

Under the draft Guidelines, data subjects would have broad rights in relation to their personal information held by data processors, including:

(a) **Right to confidentiality**

The data processor should not disclose personal information to any natural person or legal entity for purposes other than those notified to the data subject.

(b) **Right to knowledge**

The data subject would have the right to receive accurate information on the content of his or her personal information, the source of that information, the purpose and scope of use, and the scope of disclosure to third parties.

(c) **Right to opt out, change data or prohibit use**

Data subjects would have the right to accept or refuse to provide personal information, the right to request data processors amend or correct personal information which is incomplete or inaccurate, and the right to request data processors stop processing and delete personal information.

Prohibition on collecting personal information of children without their guardian's consent

Data processors would be generally prohibited from collecting personal information from / or about people under 16 years of age. In the event that the collection of such information is necessary to provide services, consent from the child's guardian would have to be obtained.

Irrelevant personal information should not be collected

The Guidelines prohibit data processors from collecting information which is not directly connected to the stated purpose, especially information relating to ethnicity, religious belief, genetic information, fingerprints, health condition or sex life.

Transferring personal information

The draft Guidelines take a restrictive position on the transfer of personal information between data processors and could create difficulties for multinational corporations relying on third party data processing companies or routinely passing information between affiliates.

(d) Presumption against transfer to third parties

The draft Guidelines generally prohibit transfer of personal information to third parties. In situations where personal information would be transferred to third parties, the data processor would have to disclose the identity of the transferees and obtain consent from the data subject.

(e) Presumption against allowing cross-border transfer of personal information

Under the draft Guidelines, transferring personal information to foreign data processors is prohibited except where there are clear laws or regulations permitting the transfer or the industry regulator has agreed. Given the lack of current PRC laws and regulations on this subject, the proposed rule could have a major impact on companies using offshore data centers or transferring information to foreign affiliates, especially in the financial services and insurance industries, where collection and transfer of personal data is necessary for business operations.

In this respect, the position in the draft Guidelines is far more restrictive than the proposed Draft Privacy Law, which would generally allow international transfer of information subject to informed consent, national security considerations and the adequacy of data privacy laws in the recipient's jurisdiction.

(f) Use of personal information following mergers or acquisitions

The draft Guidelines require that in the event a data processor is involved in a merger or acquisition, the transaction documents would have to specify that the use and level of protection of personal information would not change.

COMMENTARY

The preface to the draft Guidelines notes that a number of domestic internet and software companies and industry associations were consulted in the course of preparing the draft, and the text appears to have been primarily prepared considering online collection of data from internet

users. However, the draft Guidelines would potentially apply to virtually any company: for example, employers with digital records on employees, or financial institutions and insurers with records on their customers. While the general principles relating to informed consent and consumer protection are reasonable, the extent of proposed restrictions on transfer of personal information between entities and internationally could unnecessarily raise compliance costs. As further steps are taken toward enacting regulations on personal data privacy, regulators should consider the practical costs of implementation and the wider impact that rules in this area will have on companies doing business in the PRC.

Gastón Fernández (Associate), gaston.fernandez@hoganlovells.com, Hogan Lovells, Beijing, PRC