(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**	18 of 2012	01/10/2012

(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 or any other Ordinance. (Amended 18 of 2012 s. 13)

(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; (Amended 18 of 2012 s. 13)

(ea) the data user is entitled under this or any other Ordinance not to comply with the request; or (Added 18 of 2012 s. 13)

(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 8 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.

(5) Despite any provision in any relevant Ordinance or its subsidiary legislation in relation to discovery and inspection, in any proceedings under this Ordinance, a specified body—

(a) may, for the purpose of deciding on the issue as to whether a data user is required or entitled to refuse to comply with a data access request under this section or deciding on any question related to that issue, require the personal data which is the subject of the request to be made available for its inspection; and

(b) must not require the personal data to be disclosed to any party to the proceedings, whether by discovery or otherwise, unless it has decided that the data user must comply with the request. (Added 18 of 2012 s. 13)

(6) In subsection (5)—

proceedings under this Ordinance (根據本條例進行的法律程序) has the same meaning given by section 13(4); ***relevant Ordinance*** (有關條例) means—

(a) the High Court Ordinance (Cap 4);

(b) the District Court Ordinance (Cap 336); or

(c) the Administrative Appeals Board Ordinance (Cap 442);

specified body (指明當局) has the same meaning given by section 13(4). (Added 18 of 2012 s. 13)

(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)

Part: 5 Division: 2	**Correction of Personal Data**	18 of 2012	01/10/2012

(Added 18 of 2012 s. 14)

Section:	22	**Data correction request**	18 of 2012	01/10/2012

(1) Subject to subsections (1A) and (2), where- (Amended 18 of 2012 s. 15)

(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 is inaccurate, (Amended 18 of 2012 s. 15)

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.

(1A) If a person is a relevant person in relation to an individual only because the person has been authorized in writing by the individual to make a data access request on behalf of the individual, the person is not entitled to make a data correction request. (Added 18 of 2012 s. 15)

(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 is the subject of a data correction request still under consideration by the user (or words to the like effect). (Amended 18 of 2012 s. 15)

(4) A person who, in a data correction request, supplies any information which is false or misleading in a material particular for the purpose of having the personal data corrected as indicated in the request, commits an offence and is liable on conviction to a fine at level 3 and to imprisonment for 6 months. (Added 18 of 2012 s. 15)

(Enacted 1995)

Section:	23	**Compliance with data correction request**	18 of 2012	01/10/2012

(1) Subject to subsection (2) and section 24, a data user who is satisfied that personal data to which a data correction request relates is inaccurate shall, not later than 40 days after receiving the request- (Amended 18 of 2012 s. 2)

(a) make the necessary correction to the data;

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

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

(i) the data has 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 the data for the purpose (including any directly related purpose) for which the data was disclosed to the third party,

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

(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,

is exempt from the provisions of data protection principle 6 and section 18(1)(b)- (Amended 18 of 2012 s. 2)

(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**	18 of 2012	01/10/2012

(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 is 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. (Amended 18 of 2012 s. 2)

(2) Personal data is exempt from the provisions of data protection principle 3 in any case in which- (Amended 18 of 2012 s. 2)

(a) the use of the data is for any of the purposes referred to in subsection (1) (and whether or not the data is held for any of those purposes); and (Amended 18 of 2012 s. 2)

(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 is or has 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; 18 of 2012 s. 2)

(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.**	18 of 2012	01/10/2012

(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), is 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- (Amended 18 of 2012 s.31)

(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 is exempt from the provisions of data protection principle 3 in any case in which- (Amended 18 of 2012 s. 31)

(a) the use of the data is for any of the purposes referred to in subsection (1) (and whether or not the data is held for any of those purposes); and (Amended 18 of 2012 s. 31)

(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.

(6) In this section—

crime (罪行) means—

(a) an offence under the laws of Hong Kong; or

(b) if personal data is held or used in connection with legal or law enforcement cooperation between Hong Kong and a place outside Hong Kong, an offence under the laws of that place;

offender (犯罪者) means a person who commits a crime. (Added 18 of 2012 s. 31)

(Enacted 1995)

Section:	58A	**Protected product and relevant records under Interception of Communications and Surveillance Ordinance**	18 of 2012	01/10/2012

(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 is, or is contained in, protected product or relevant records. (Amended 18 of 2012 s. 2)

(2) Personal data which is, or is contained in, protected product or relevant records is exempt from the provisions of this Ordinance. (Amended 18 of 2012 s. 2)

(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).

of this right of choice (i) when soliciting the personal data in question; and (ii) in the response channel through which the data subject may elect to give his/her consent.

2.17 In some circumstances, a data user may seek a general consent from the data subjects to cover all specified kinds of personal data, classes of marketing subjects and classes of persons to which the data is to be provided. If no such consent is given by the data subject, a data user is not allowed to use any kind of personal data of the data subject to market any class of products or services or provide any personal data of the data subject to any class of persons for use in direct marketing.

Tips:

1. Do not ask customers to provide bundled-consent. Service-providers should obtain customers' consent for the use and/or provision of their personal data to others for use in direct marketing separately from the agreement and acceptance to the use of their personal data in connection with the services offered to them
2. Allow customers to indicate separately whether they agree to (i) the use, and (ii) the provision of their personal data to others
3. Provide information to customers in one self-contained document and avoid making cross-reference to other documents or other sources of information as far as practicable
4. Provide a check-box for customers to indicate agreement or no objection to the use of personal data for promotion of products and services
5. Inform customers that they may give selective consent to (a) the kinds of personal data; (b) the classes of marketing subjects; and (c) the classes of data transferees
6. Highlight check-boxes to attract customers' attention and use simple, easily understandable and readable language

Use of the personal data

2.18 Data users are required under DPP3 not to use personal data for a new purpose unless the prescribed consent is obtained from the data subject. A new purpose means a purpose other than the purpose for which the data was to be used at the time of the collection or a directly related purpose. Under section 2(3), prescribed consent means express consent given voluntarily which has not been withdrawn in writing.

2.19 In accordance with DPP3, if a data user intends to use or provide personal data for use in direct marketing, it has to seek the prescribed consent from the data subject if such data was originally collected not for direct marketing purpose. Despite section 2(3), a data user is taken to have obtained the prescribed consent of the data subject if it has not contravened any of the relevant provisions regarding (i) the taking of specified actions before using or providing personal data for use in direct marketing; (ii) not using or providing personal data for use in direct marketing without the data subject's consent; and (iii) ceasing the use or provision of personal data for use in direct marketing upon obtaining an opt-out request from the data subject[16]. These requirements [(i), (ii), and (iii)] are explained in Parts 3 and 4.

[16] Sections 35H and 35M

PART 3

USE OF PERSONAL DATA IN DIRECT MARKETING

New requirements to be followed before using personal data in direct marketing

3.1 A data user who intends to use a data subject's personal data in direct marketing must take specified actions which are elaborated below. The obligation on the data user applies irrespective of whether the personal data is collected from the data subject by the data user[17]. Hence, even if a data user has collected the personal data of a data subject from a third party, it is still required to take the specified actions and obtain the necessary consent[18] from the data subject before using the personal data for direct marketing.

Inform the data subject of data user's intention to use the personal data in direct marketing and provide the data subject with the prescribed information

When to inform?

3.2 As a responsible approach, it is always advisable for the data user to inform the data subject as early as possible the data user's intention to use the data subject's personal data for direct marketing purpose. Where possible, this should be done on or before the personal data of the data subject is collected.

Example of notification:

When a customer opens a savings account with a bank, the customer should be informed of the bank's intention to use his personal data for marketing its different types of banking services and be given a choice of whether to allow such usage at the time his personal data is collected.

3.3 General and loose description of the purpose of use such as *"such other purposes as the company may from time to time prescribe"* will not be acceptable.

What to be included?

3.4 The following information must be included in the notice to the data subject:

(a) The data user intends to use the personal data of the data subject for direct marketing;

(b) The data user may not so use the data unless the data user has received the data subject's consent to the intended use;

(c) The kinds of personal data to be used;

(d) The classes of marketing subjects in relation to which the data is to be used; and

[17] Section 35C(3)

[18] The definition of "consent" includes "an indication of no objection" (see section 35A(1)).

user intends to use the personal data in direct marketing, it is prudent for data users to provide the information by way of a written notice which is generally referred to as "Personal Information Collection Statement" ("**PICS**").

*PICS and Privacy Policy Statement ("**PPS**")*

2.9 PICS and PPS are common tools for data users to communicate their purpose(s) of collection of personal data, the kinds of data collected, the possible classes of transferees of the data as well as the policies and practices in relation to personal data. They serve as evidence to demonstrate that practical steps have been taken by a data user to provide the information to the data subjects.

2.10 To ensure that a PICS is effective, it is necessary for data users to take into consideration the following factors:

(a) Whether the layout and presentation of the PICS (including the font size, spacing, underlining, use of headings, highlights and contrasts) has been designed so that the PICS is easily readable to customers with normal eyesight.

(b) Whether the PICS is presented in a conspicuous manner (e.g. the PICS is a stand-alone section and its contents are not buried among the terms and conditions for the provision of the data user's services).

(c) Whether the language used in the PICS is easily understandable (e.g. the choice of simple rather than difficult words and the avoidance of use of legal terms or convoluted phrases).

(d) Whether further assistance from the data user such as help desk or enquiry service is available to enable the customer to understand the contents of the PICS.

2.11 Data users should communicate their message effectively in clear and simple language and in a form easily understandable, readable and accessible by reference to the actual circumstances under which the personal data is collected such as the characteristics of the targeted customers (in terms of age, education level, etc.).

2.12 Data users should not define the purpose of use and class of transferees of the personal data in such liberal and vague terms that it would not be practicable for customers to ascertain with a reasonable degree of certainty how their personal data could be used and who could have the use of the data.

2.13 If a data user intends to use or provide personal data for use in direct marketing, it must inform the data subjects that it intends to so use or provide the data and that the data may not be so used or provided unless it receives the data subject's consent (in the case of provision of personal data, the consent must be in writing) to the intended use or provision[13]. More elaboration on the information to be provided to the data subject will be discussed below and under Part 3.

[13] Sections 35C(2) and 35J(2).

Tips for defining purpose of use and class of transferees:

✗ Avoid using loose terms, for example, *"such other purposes as the Company may from time to time prescribe"* to cover direct marketing as a purpose of collection.

✓ An effective way is to define the class of transferees by its distinctive features, such as *"financial services companies"*, *"investment service providers"*, *"telecommunications services providers"*, etc.

✗ Avoid using vague terms such as, *"all business partners"*, *"selected companies which will provide information of services in which customers may be interested"* or *"such other agents as the company may from time to time appoint"*.

Obtain consent on application forms

2.14 Data users are reminded **NOT** to design a service application form in such a way that renders it impracticable for its customers to refuse the use of their personal data for direct marketing purposes. For example, it is common for a service application form to incorporate both the terms and conditions of provision of the data user's services as well as statements relating to the use of the data collected for marketing products or services, or the provision of the personal data to a third party. If the customer is only provided with one space to sign on the form, he has to choose between (a) giving up the application for the service or (b) giving his "bundled consent" agreeing to the terms and conditions for the provision of the service he originally seeks as well as the use of his personal data as prescribed by the data user when in fact he finds such prescribed use objectionable. This is undesirable.

2.15 In such circumstances, the data user is advised to design its service application form in a manner that provides for the customer's agreement to the terms and conditions for the provision of the service to be separated from the customers' consent to the use of his personal data for direct marketing. Recommended ways to achieve this end include providing a separate signature or tick box to indicate the customer's agreement or no objection to the prescribed use of his personal data.

General or selective consent[14]

2.16 A data subject's consent for the use or provision of his/her personal data for use in direct marketing may be given either *generally or selectively*[15]. By selective consent, the data subject may choose to restrict his/her consent to (a) only certain kinds of personal data held by the data user; (b) only certain classes of the full range of marketing subjects offered by the data user; and/or (c) only certain classes of persons to which the data user intends to provide for use in direct marketing. To facilitate the data subjects' exercise of their choice, it is recommended that data users inform the data subjects

[14] The definition of consent includes an "indication of no objection".

[15] Sections 35E(1)(a) and 35K(1)(a)