Appendix II

Departmental Guidelines for the Compliance with the Personal Data (Privacy) Ordinance

Annexes (to be updated when required)

A Data Protection Principles

B Sample Personal Information Collection Statement (with Chinese translation)

C Sample Authorisation Statement (to obtain prescribed consent for data matching) (with Chinese translation)

D Sample Personal Information Collection Statement for Collecting Witness Statements (with Chinese translation)

E Exemptions – A Summary

F Guidelines for Handling Requests for Personal Data from Other Departments/Public Bodies

G Memo from Secretary for Home Affairs of 28 November 1996 on Compliance with Personal Data (Privacy) Ordinance

H Memo from Secretary for Home Affairs of 16 April 2002 on Guidelines on Processing Requests for Information for Civil Proceedings

I General Security Guidelines for Handling Personal Data

J Standard Fee for Providing Personal Data

K Administrative Procedures for Data Access Request

L Administrative Procedures for Data Correction Request

M Sample Format of Record of Refusals of Data Access and Correction Requests

I. INTRODUCTION

Background and Overall Objectives of the Ordinance

The Personal Data (Privacy) Ordinance, Cap 486 (the Ordinance) was enacted on 3 August 1995, became operative on 20 December 1996 and was amended on 1 October 2012. Generally speaking, the Ordinance governs the collection, accuracy, retention, use and security of personal data by data users and enables individuals to request access to and correction of any personal data relating to them. The purpose of the Ordinance is to protect the privacy interests of living individuals in relation to personal data. It also contributes to Hong Kong's continued economic well being by safeguarding the free flow of personal data to Hong Kong from restrictions by countries that already have data protection laws. It is applicable to all bodies in both the public and private sectors that control the collection, holding, processing or use of personal data.

2. The Ordinance establishes an independent statutory office to enforce and promote compliance with the provisions of the Ordinance by the name of the Privacy Commissioner ("Privacy Commissioner") for Personal Data.

Some Useful Definitions

3. The following definitions are useful for the purpose of this set of guidelines:

Personal data means any data relating directly or indirectly to a living individual, from which it is practicable to ascertain the identity of the individual and which are in a form in which access or processing is practicable.

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

Data user means a person who controls the collection, holding, processing or use of the personal data.

A **Matching procedure** comprises **all** the following elements :

(a) the comparison of 2 sets of personal data, which are collected for different purposes;

(b) checking involves the personal data of 10 or more data subjects;

(c) comparison is not carried out by manual means;

(d) the comparison is for the purpose of producing or verifying data that may be used for the purpose of taking adverse action against any of those data subjects.

Relevant person of the data subject means

(a) where the data subject is a minor, a person who has parental responsibility for the minor;

(b) where the data subject is incapable of managing his own affairs, a person who has been appointed by a court to manage those affairs;

(c) where the individual is mentally incapacitated within the meaning of section 2 of the Mental Health Ordinance (Cap 136)-

  (i) a person appointed under section 44A, 59O or 59Q of that Ordinance to be the guardian of that individual; or

  (ii) if the guardianship of that individual is vested in, or the functions of the appointed guardian are to be performed by, the Director of Social Welfare or any other person under section 44B(2A) or (2B) or 59T(1) or (2) of that Ordinance, the Director of Social Welfare or that other person.

Prescribed consent means the express consent of the person given voluntarily.

Data Protection Principles (DPPs)

4. The Ordinance places a statutory duty on data users to comply with the requirements of the six DPPs as set out in Schedule 1 to the Ordinance. All officers who have responsibility for handling personal data or managing personal data systems should familiarise themselves with these six DPPs on the following areas:

(a) Principle 1 - purpose and manner of collection of personal data
(b) Principle 2 - accuracy and duration of retention of personal data
(c) Principle 3 - use of personal data
(d) Principle 4 - security of personal data
(e) Principle 5 - information to be generally available
(f) Principle 6 - access to personal data

5. The six DPPs are reproduced at **Annex A**.

Code of Practice

6. The Privacy Commissioner is authorised to issue Codes of Practice for the purposes of providing practical guidance in respect of any requirements under the Ordinance imposed on data users, e.g. Code of Practice on the Identity Card Number and other Personal Identifiers. All data users are required to observe the guidelines as stipulated in these Codes. Though failure to comply with the provisions of a Code may not by itself render a data user liable to civil or criminal proceedings, a breach of the Codes by a data user will give rise to a presumption against the data user in any legal proceedings under the Ordinance, including criminal proceedings under the Ordinance. Failure to observe a Code by a data user will also weigh unfavourably against the data user in any case before the Privacy Commissioner.

7. A number of Codes have been published by the Privacy Commissioner, which include : (a) the Code of Practice on the Identity Card Number and Other Personal Identifiers which provides guidance on the appropriate handling of personal identifier in general and handling of Identity Card Numbers and copies of ID Cards in particular; (b) The Code of Practice on Human Resource Management, which provides employers and HRM practitioners with a practical guide about the application of the provisions of the Ordinance to the employment-related personal data privacy and application of the DPPs to the management of personal data in three important areas, namely recruitment, current employees and former employees. These Codes of Practice published by the Privacy Commissioner can be downloaded from the Office of the

Privacy Commissioner's web site at [http://www.pcpd.org.hk].

Offences

8. Data users are under a statutory duty not to engage in any act or practice that contravenes a DPP unless required or permitted under the Ordinance.

9. For any contravention of the requirement under the Ordinance (which includes any case where the data user has done an act or engaged in a practice in contravention of a DPP), complaints may be made to the Privacy Commissioner. The Privacy Commissioner may serve an enforcement notice ("EN") for compliance with the requirement.

10. Generally, it is an offence if a data user, without reasonable cause, contravenes any requirement (other than a DPP) under the Ordinance [S.64A]. Various other offences are also stipulated under the Ordinance, including the following which may be more relevant to HA's general operation –

(a) contravention of an EN [S.50A(1)];

(b) having complied with an EN, intentionally does the same act or makes the same omission in contravention of the requirement under the Ordinance as specified in the EN [S.50A(3)];

(c) disclosing any personal data of a data subject obtained from a data user without the latter's consent and with an intent to (a) obtain gain for himself or another person, or (b) cause loss to the data subject [S.64(1)];

(d) disclosure of personal data of a data subject without the data subject's consent, causing psychological harm to the data subject [S.64(2)];

(e) supplying any information which is false or misleading in a material particular in a data access request [S.18(5)];

(f) supplying any information which is false or misleading in a material particular for the purpose of obtaining the Privacy Commissioner's consent to the carrying out of matching procedures [S.31(4)];

(g) contravention of any conditions specified in the Privacy Commissioner's consent to the carrying out of matching procedures [S.32(5)]; and

(h) failure to comply with the requirements of the Privacy Commissioner or officers in performance of functions under the Ordinance or making any false or misleading statement in connection therewith [S.50B];

11. Provision is also made under the Ordinance for an individual who suffers damage by reason of a contravention of the requirement of the Ordinance in relation to his/her personal data to obtain compensation from the data user concerned.

II. DEPARTMENT'S POLICY ON PERSONAL DATA

Departmental Policy on Personal Data

12. The Housing Authority/ Housing Department is committed to launching a Privacy Management Programme as part of its corporate responsibility. We take personal data privacy protection not merely as a compliance issue but also as part of our corporate governance responsibilities and apply it as a business imperative. All employees of the Housing Authority and the Department must bear in mind that, when collecting, using, handling, storing and transmitting personal data, the interests of individual data subjects should be a primary concern. Special care must be taken to safeguard against unauthorised use or disclosure of personal data.

Statement of Privacy Policy and Practices

13. HA/HD has published its Privacy Policy Statement in its website at http://www.housingauthority.gov.hk/. A hard copy of the Statement is on display in the public reading area of the Housing Authority Library on 4/F, Block 3 of the Housing Authority Headquarters Building. For details about the Statement, please refer to paragraph 24 of Appendix I of this circular.

III. THE COLLECTION, ACCURACY, RETENTION, USE AND SECURITY OF PERSONAL DATA

Data Collection

14. The means by which personal data are collected may include the use of printed forms, face to face or telephone interviews to obtain data about an individual from the data subject himself/herself, another person or an organisation. Means of data collection should be lawful and fair. For all personal data collected through all forms/channels, the purposes of data collection should be identified and clearly stated. Unnecessary data should not be collected.

15. For each means of collection, where personal data are collected from the data subject directly, arrangements should be made to inform the data subject on or before the collection of data the followings:

(a) whether it is obligatory or voluntary for the data subject to supply the personal data. In the case of the former, the consequences if he/she fails to supply the data. If providing the personal data is not obligatory, then the question of whether the data should be requested at all has to be considered;

(b) the purpose(s) of collection of personal data;

(c) the classes of persons to whom the data may be transferred for the purpose(s) identified;

(d) the rights of the data subject to request access to and correction of the personal data; and

(e) the name and address of the officer in the Department to whom the above requests may be made. Requests for access to personal data made under the Ordinance could be made to the Departmental Data Protection Officer ("DDPO"), or wherever practicable, to the data user office if it will be more convenient for the data subjects to contact the data user direct for handling the request through the normal course of business.

16. Acceptable arrangements for informing data subject of the above matters include printing the Personal Information Collection Statement (PICS) on the forms used to collect the personal data or on separate slips attached to the forms. Displaying a notice at the location where the personal data are collected is also a means of informing the data subject. However, it is not advisable to rely solely on displayed notices unless the notices are displayed at the point of collection and physical attendance of the data subject is required on collection of the data or the document containing the data. Rather, displaying notices should be used as a supplementary measure to inform the data subject. It is also considered a good management practice to verbally inform the illiterate or the elderly of the PICS. According to the "Preparing On-line Personal Information Collection Statements and Privacy Policy Statements" issued by the Privacy Commissioner, a PICS should be provided when personal data are collected on-line from data subjects. Besides, it is a good practice to make available an on-line Statement of Privacy Policy and Practices.

17. A draft sample PICS for compliance with the requirements in paragraph 15 is at **Annex B**. The sample PICS should not be taken as standard or mandatory provisions and are meant for reference only. Taking into account different purposes for collection of personal data and different operational needs, the data user should carefully define the purpose of data collection in a sufficiently broad manner so that the immediate purpose as well as all possible legitimate purposes are covered in the PICS. The data users should carefully review existing standard forms in use in order to distinguish forms for collection of personal data from forms containing mere undertakings from the applicants and which do not involve provision of personal data. In the latter case, the PICS may not be required to be incorporated.

18. For administrative convenience, these PICSs can be incorporated in the main or master forms which are the first approach of data collection. Acknowledgement of the PICS however is not mandatory so long as practicable steps have been made to communicate the matters in paragraph 15 to the data subject.

19. Where personal data are collected repeatedly from a data subject and there is no material change in the matters required to be communicated to the data subject under paragraph 15 above, it is not

required to repeat the communication of the matters to the data subject if not more than 12 months have elapsed between the first collection and the subsequent collection. Nevertheless, if the subsequent data collection takes place after 12 months from the first data collection, the data subject should be reminded of the matters again by either expressly making it known to the data subject or referring to him the PICS stated on the main or master forms.

20. For information collected at interviews where the data are recorded and the data subject is not required to sign the record, the data subject should be expressly informed of the matters in paragraph 15 above and a note should be recorded to the effect that the matters in paragraph 15 above have been properly explained to the data subject.

21. In case subsequent collection of personal data from third parties or data matching about the data subject is required for the purpose(s) stated, it is advisable to obtain authorisation from the data subject at the time of data collection. A sample authorisation is at **Annex C** for reference. The authorisation may be incorporated as part of the data collection form. If the form contains personal data other than that of the data subject himself, and data matching is required in respect of such other personal data, separate authorisation from each other individual involved is required. Witnessing of the authorisation is not mandatory.

22. For **business associate**[1] personal data, the following steps should be observed:

(a) identify which of the data are regarded as personal data for the purpose of the Ordinance. If no personal data are involved, the provisions of the Ordinance will not apply;

(b) in case personal data are involved, ensure that personal data should only be collected for a lawful purpose and directly related to the Department's functions and activities through lawful and fair means;

(c) if personal data are involved, determine whether the

[1] For definition of business associate personal data, please refer to Annex 1 to Appendix I of this Circular.

person from whom the personal data are collected is the data subject;

(d) if the personal data are not collected from the data subject, e.g. if the personal data are collected from the business associates and not directly from the individuals concerned, DPP1 in respect of collection of personal data is not required to be followed. In other words, there is no requirement under the Ordinance to inform the data subject the matters listed in paragraph 15 above. However, it is considered a good administrative practice to inform the business associates concerned the purpose of collecting the personal data. Most of the business associate personal data should fall into this category; and

(e) if the business associate concerned is a sole proprietorship, any personal data collected from the proprietor may be considered as directly collected from the data subject.

Data Accuracy

23. There should be arrangements for checking and updating personal data so as to ensure that personal data kept are accurate having regard to the purpose of the use of the data.

24. In case the data subject is required to inform the Department of any changes in his/her personal data, this should be expressly communicated to the data subject, e.g. through the data collection forms.

Data Retention

25. Personal data, including customer and business associate personal data, are mainly kept under three modes of storage, namely, in the form of paper files, computer files, and microfilm.

26. For whatever means of data storage, steps should be taken to ensure that arrangements for disposing of obsolete records meet the requirement that personal data shall not be kept longer than is necessary for the purposes they are used for. These purposes are the purposes for which the data were collected, any other directly related purposes, and any other purposes to which the data subject has voluntarily given express consent.

27. Both Section 26 and DPP2 of the Ordinance require the data users to erase personal data which are no longer required after fulfillment of the original stated purpose of collection. The retention period for each mode of storage should be critically reviewed by relevant data owners based on their operational needs. This is particularly necessary for those files relating to ex-tenants and unsuccessful applicants for various housing schemes. Consideration should be given to keeping only the necessary portion of file record, instead of the whole file record.

28. Notwithstanding the above requirement, personal data can be retained where:

(a) erasure is prohibited under any law; or

(b) it is in the public interest not to erase the data. The public interest here includes historical (archival) interest.

Data Use

29. DPP3 requires that, unless with the prescribed consent of the data subject, personal data shall only be used for the purpose for which they were collected or for a directly-related purpose. In other words, the purpose specified to the data subject at the time of the collection will limit the future use of the personal information collected. Disclosure of personal data to external bodies for any purpose other than the purpose for which the data were to be used at the time of the collection or for a directly-related purpose, is also governed by the restriction of DPP3. Use of the data for another purpose without the data subject's prescribed consent may amount to breach of the DPP3.

30. The Ordinance empowers a specified third party to give consent, on behalf of minors, persons incapable of managing their own affairs, or mentally incapacitated persons, to the change of use of their personal data when it is clearly in their interests to do so. The third parties specified for these classes of data subjects are respectively a person who has parental responsibility for the minor, a person appointed by court to manage the data subject's affairs, and a person appointed to be guardian of the data subject under the Mental Health Ordinance.

Use of Complainant's Personal Data Collected in Public Complaints

31. Our department may receive complaints from members of the public direct or through other departments or agencies. In the course of handling these public complaints, personal data of the complainant may be collected. These data may include the name and contact means like telephone number and address of the complainants and other information etc. To comply with the requirements under DPP1(3), if practicable, arrangements should be made to inform the complainant, on or before collecting data from him, of the points set out in paragraphs 15(a) to (e) above. An example of acceptable arrangement is the provision of a PICS.

32. In handling personal data collected in public complaints, the purpose for the collection of personal data, e.g. the purpose stipulated in the PICS or verbal notice, will govern the future use of the complainant's data. Hence, all complaints should be treated in confidence and the identity and personal data of the complainant should be kept confidential.

In general, the complainant's data should be used for processing of the complaint and directly related purpose. If the subsequent use is not for the same purpose, or a purpose directly related to the original collection purpose, officers should not disclose/transfer any personal data of the complainant without the complainant's prescribed consent, unless an applicable exemption applies.

Collecting and Handling Witness Statements

33. From time to time, it is necessary to collect witness statements from members of the public, officers within the Department, or officers of other departments in connection with investigation and prosecution of cases related to, for example, false declaration, providing false information in applications, breach of tenancy agreement, and misconduct of staff. Such statements may contain personal data of the statement provider or other parties. When collecting witness statements and handling personal data contained therein, officers should observe the principles stipulated in these guidelines.

34. For the purpose of satisfying the requirement set out in DPP1(3), the officer should provide a PICS to the witness. A sample PICS for collecting witness statements is at **Annex D** for reference. Section Heads may vary the wordings of the sample PICS to suit their need so long as the points set out in paragraphs 15(a) to (e) of these guidelines are covered. It is advisable to append the PICS to the witness statement.

35. The subject officer should also inform the witness of the content of the PICS before taking the witness statement. If the witness is illiterate or elderly, the officer collecting the statement should ensure that the witness understands the content of the PICS.

36. Where a witness statement is collected at the request of the Prosecutions Section of the Legal Service Sub-division for prosecution of offences, the officer concerned will be informed by the Prosecutions Section of the steps to follow in obtaining the witness statement. The officer must comply with all such steps.

37. Since DPP 3 provides that without the prescribed consent of the data subject, personal data shall not be used for any purpose other

than the purpose for which they were collected or for a directly-related purpose, in general, any request for release of a witness statement should be dealt with in accordance with the principles laid down in these guidelines. For prosecution cases, while prosecution action is in progress, a prosecutor has a duty to disclose to the accused, upon the latter's request, all materials in his possession which constitute evidence relevant to the guilt or innocence of the accused. Such materials may include witness statements. For those prosecution actions instituted by the Prosecutions Section, officers receiving any such request from the accused should refer it to the Prosecutions Section for handling. For other prosecution actions, officers should refer the request to the relevant prosecution authority. Officers must not release any information in witness statements to the accused without the agreement of AD(LS). Whenever in doubt, officers should contact AD(LS) for advice.

Use of Personal Data in Direct Marketing

38. Part 6 of the Ordinance requires a data user who intends to use or provide the personal data of a data subject to others for use in direct marketing to inform the data subject of certain prescribed information and provide the data subject with a response channel through which the data subject may indicate whether he objects to the intended use or provision. The prescribed information can be provided to the data subject either orally or in writing. However, the provision of personal data (whether for gain or not) to another data user will be subject to the requirement that the data user must provide to the data subject in writing the prescribed information. For guidelines on direct marketing, data users should refer to the "New Guidance on Direct Marketing" which was published by the Privacy Commissioner and can be downloaded at [http://www.pcpd.org.hk] under "*publications and videos*".

Data Transfer

39. In case data transfer outside the Department is necessary for the purpose of data collection, data subject should be expressly informed of the classes of persons/organisations to whom/which the data may be transferred (i.e. classes of transferees). Consent should preferably be obtained from the data subject at the time of data collection.

40. Data transfer is found to be common in handling **customer personal data.** If it is considered that a list of classes of transferees could not be exhausted, a general statement should be added in the PICS to the effect that the data may be transferred to other Government Departments for the stated purpose(s) of collection to cater for this type of usual transfer.

41. It is not common to transfer **business associate personal data** outside the Department. In case such a transfer is required, the consent of both the business associates and the individuals concerned should be sought.

42. All data users in the Department in control of any personal information that was collected for certain stated purpose shall refuse to disclose the information to external bodies, **unless**:

(a) the purpose for which the information is to be used is the same or directly related to the purpose for which the information was collected; or

(b) the individual to whom the data relates has given consent voluntarily to the use of his/her personal data for other altered purpose; or

(c) the use of the personal data without prior consent of the data subject concerned is required or authorised by or under law; or

(d) there is an applicable exemption from DPP3 under the Ordinance and the data user has reasonable ground(s) to believe that strict adherence to DPP3 would likely be prejudicial to certain exempted interests referred to in Part VIII of the Ordinance which are summarised at **Annex E** (see also paragraphs 83 to 85).

43. A distinction should be made between a mandatory disclosure which is required by legislation and a discretionary disclosure under applicable exemption. If there is doubt about the statutory power under which the requesting party requires any specific personal data to be disclosed, the subject officer should ask the requester to confirm/clarify whether the provision of the requested personal data is obligatory and under which specific statutory authority.

44. It should be reminded that the Ordinance does not require the data user to disclose personal data without consent of a data subject, even if there is an applicable exemption. The data user is entitled not to disclose personal data in the absence of a legal obligation to do so. Whatever circumstances exist that would permit disclosure without consent by relying on any applicable exemption, it must be narrowly defined and strictly limited for balancing the competing public interests and appropriate protection of personal data. The subject officer should ask the requestor to state the exemption he relies on and gives reasons to justify his claim of an exemption. The subject officer should seek legal advice if in doubt about the applicability of the exemption.

45. If the relevant exemption is claimed, the data user should examine whether our failure to permit the disclosure/use of the personal data would be likely to prejudice any matter referred to in the relevant exemption. The requesting party should bear the burden of proof in respect of their requests for access, with or without consent of the data subjects. It should be noted that it is the disclosing party who will need to rely on the defence of the exemption for protection against any possible future claims from any person for a contravention of the DPP3.

46. Prior to releasing personal data by relying on an applicable exemption, proper authorisation should be obtained. The decision to release personal data without consent of the data subject by claiming exemption should be authorised by a subject officer not lower than professional level or equivalent.

47. The guidelines for handling requests for personal data from other departments/public bodies are at **Annex F**. This is to assist officers handling requests for **customer data** in particular. Besides, due regard should be made to the principles set out in the memo of the Secretary for Home Affairs of 28 November 1996 at **Annex G**. In view of an increasing number of requests for personal data from members of the public or their legal representatives alleging that they require the data to institute civil proceedings to prevent or remedy unlawful or improper conducts, HAB has drawn up the guidelines on processing requests for information for civil proceedings at **Annex H**. Officers handling such requests must exercise their best judgement in each individual case.

Data Security

48. In compliance with DPP4, practicable steps should be taken to ensure that the personal data held are subject to appropriate security conditions. In determining such conditions, due regard should be given to:

(a) the kind of personal data and the harm that could be caused by unauthorised or accidental access, processing, erasure, loss or use. Security efforts would be in proportion to potential for damage;

(b) the physical location of the data (e.g. whether there are controls on access to the place where the data are located);

(c) security measures incorporated into the equipment in which the data are stored (e.g. the use of passwords to access computer data bases);

(d) measures taken to ensure the integrity, prudence and competence of persons having access to the data; and

(e) measures taken to achieve secure transmission of the data.

49. Data users should review on the security arrangements of handling of the personal data periodically to ensure that personal data is

protected from unauthorised use or accidental leakage.

50. Some general security guidelines for handling personal data are at **Annex I**. Data users may also make reference to DGC No. 9/2005 on "Security of Official Information and Building" and ITC No. 3/2008 on "Guideline on Security Measures concerning Personal or Restricted Data for use Outside Housing Department Office Environment". For query in respect of DGC No.9/2005 and ITC No. 3/2008, please contact Departmental Security Officer (Chief Executive Officer/Administration) at 2761 6168 and ITM/8 at 2761 6316 respectively.

Data Matching

51. Automated data comparison, which meets all of the four criteria referred in the paragraph 3 of these guidelines will be a Matching Procedure and be regulated by Sections 30-32 of the Ordinance. If such data matching is required, either the prior prescribed consent of all the individual subjects or prior approval of the Privacy Commissioner has to be sought. Consent from the data subject should preferably be obtained at the time of data collection (see sample authorisation at **Annex C**). For seeking the approval from the Privacy Commissioner, a Consent Application Form for carrying out matching procedures should be completed. The data user is required to comply with the conditions of the matching approval and furnish reports to the Privacy Commissioner for renewal of the approval in a timely manner.

52. Data sharing will occur between data users collecting personal information for different purposes. Matching approval from Privacy Commissioner may still be required even if the two different sets of personal data are collected by the same organisation. Comparison of data collected in different occasions and for different purposes, if not within the scope of a Matching Procedure, may potentially be restricted by the DPP3. Such use or disclosure of the personal data in question is permissible with prescribed consent from the individual to whom the information relates or where there are applicable exemptions for not complying with the DPP3.

Personal Data Privacy and the Internet

53. In collecting, displaying or transmitting personal data over the Internet, data users should make reference to the guidance note on " Guidance for Data User on the Collection and Use of Personal Data through the Internet" which was published by the Privacy Commissioner and can be downloaded at [http://www.pcpd.org.hk] under "*Publications & Videos*". A reference guide for Internet users "Protecting Privacy – Using Computers and the Internet Wisely" is also available at the same web site.

Personal Data Privacy and the Surveillance of Work

54. Where employee monitoring is undertaken resulting in the collection of personal data of employees, the employer shall ensure that such act or practice complies with the DPPs. The Privacy Guidelines: "Monitoring and Personal Data Privacy at Work" provides practical guidelines for the employers to evaluate the need for employee monitoring and its impact upon personal data privacy.

IV. DATA ACCESS AND CORRECTION REQUESTS

Role of DDPO in Data Access and Correction Request Handling

55. Formal data access and correction requests made by the data subject or the relevant person under the Ordinance could be coordinated by DDPO. However, it should be emphasised that the data access right conferred upon a data subject under section 18 of the Ordinance is not to be abused nor should it be exercised to substitute or replace other proper channels for discovery of documents readily available to the data subject. For the benefit and convenience of the requester, the requester should not be indiscriminately asked to make a formal data access request, particularly when there are other proper channels for discovery of documents readily available to the data subject, or when the request for/ correction of data could be handled by the office direct through its normal business/ operation. If the requester wishes to make a formal data access, his request can be facilitated by filling in the HD 12 form. Upon receiving a form indicating a formal data access request, DDPO should make a response and refer the case to the subject office or a subject officer nominated by the divisional management for co-ordinating the returns in case the data are kept in different offices. DDPO would observe the statutory deadline for response which is 40 calendar days from the date of receipt of the request. In case the requester has not provided sufficient information to allow further processing of the request, the subject officer/ DDPO needs to ask for supplementary information from the requester. DDPO should maintain record of refusals to comply with data access and correction requests. A fee should be levied upon the requester before releasing information under a data access request.

Data Access Request

56. The Ordinance provides that an individual, or a relevant person on behalf of an individual, is entitled to make a request to:

(a) ascertain from the data user whether the data user holds personal data of which he/she 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.

Handling Data Access Request

57. The following procedures should be followed in handling data access requests:

(a) any data access request has to be responded in writing[2] and complied with within 40 calendar days after receiving the request. If the request could not be complied with, in whole or in part, within the 40-calendar days reply period, the data subject must be so informed in writing with reasons. The request should then be complied with as soon as reasonably practicable;

(b) the copy of personal data to be supplied should be such personal data as is held at the time when the request is made;

(c) if the personal data sought under a data access request are stored in more than one forms, only a copy of the data in the form or forms specified by the data subject should be provided;

---

[2] An exemption is provided to the Hong Kong Police Force to deal with data access request for criminal conviction record.

(d) if the personal data is stored in only one form and it is unable to provide a copy of the data in a form requested by the data subject (for example, the data subject requests the personal data in computerised form while the data is stored only in paper file form), a copy of such data in the available form may be provided. The data subject must be informed that this is the only form which the data can be supplied;

(e) if the personal data is stored in more than one forms, but none is the form requested by the data subject, the data subject must be informed in writing of the various forms in which the data can be supplied and that the data subject may specify within 14 calendar days the form(s) he/she would like the copy to be supplied. The data subject should be provided with a copy of the data in the form specified in his reply. If no reply is received from the data subject within 14 calendar days, a copy of the data in any appropriate form may be supplied;

(f) a copy of the personal data to be supplied should be intelligible unless it is a true copy of a document that contains the data and is unintelligible on its face. If the personal data contains any codes, they should be adequately explained such that they are readily comprehensible by the data subject, whether or not a true copy of a document is supplied;

(g) if the relevant personal data of a data access request are stored in only one language and the copy to be supplied is a true copy of the document containing such data, it is not required to provide a copy of such data in any other language. This applies even if the data subject specifies in the data access request that he/she wishes to receive the data in another language;

(h) if the personal data sought under a data access request are stored in more than one language and the

data subject specifies in the data access request that he/she wishes to receive the data in one of these languages, it is required to provide a copy of the data in the language specified by the data subject; and

(i) if it is intended to supply the personal data other than in the form of a true copy of a document, the data should be provided in either English or Chinese. The choice of English or Chinese should be made in accordance with any specific request by the data subject for one or other. In default of such a request, the choice should be made in accordance with the language used in the request.

58. A data access request shall be refused under any of the following circumstances:

(a) insufficient information is provided to identify the data subject/relevant person;

(b) it is not satisfied that the relevant person is properly authorised;

(c) the personal data requested comprises personal data of another individual, unless the consent of that other individual is available or that the request can be complied with without disclosing the identity of that other individual, for example by the omitting of names or other identifying particulars; or

(d) if compliance with the request is for the time being prohibited under this or any other Ordinance.

59. A data access request may be refused under any of the following circumstances:

(a) the request is not in writing in Chinese or English;

(b) insufficient information is provided to enable the personal data requested to be reasonably located;

(c) the request follows two or more similar requests made by the data subject or a relevant person on his behalf and it is unreasonable to comply with;

(d) another data user controls the use of the personal data concerned in such a way that prohibits the compliance of the request. For example, the Department obtains personal data from another department and that other department, in some ways, prohibits the disclosure of those personal data by the Department;

(e) the data user is entitled under this or any other Ordinance not to comply with the request; or

(f) there is an applicable exemption from subject access provided for in Part VIII of the Ordinance.

60. For the purpose of complying with paragraph 58(c) above, steps should be taken to review and amend forms that contain personal data in such a way that the part consisting of individual factual data would be separated from the part consisting of evaluative or comparative assessment relating to other individuals so that any evaluative or comparative assessment relating to other individuals could easily be excised.

61. For **customer data**, although tenancy information on household members is normally supplied by the principal tenant, a data access request from the principal tenant to obtain personal data of other household members should be supported by the consent of the other data subjects for release of the data. In case of data access request from a household member whose information is included in the tenancy application, only information relating to that particular household member should be released.

62. For the case of joint tenancy information in which personal data relating to two individuals are obtained from two separate data subjects, albeit on the same form, only the personal data of the data subject seeking access should be disclosed, unless the consent of the other data subject is available.

63. If a data access request has to be declined for any of the reasons in paragraphs 58 and 59 above, the data subject should be informed in writing of the reasons of the refusal within 40 calendar days of receiving the request. If a data access request is refused under paragraph 59(d) above, the data user is required, in the notice to the data subject, to provide the name and address of the other data user concerned.

64. A data subject or a relevant person making a data access request may be charged a fee, but this should not be excessive. Standard fees for supplying a copy of the personal data under a data access request are listed at **Annex J**. These charges will be reviewed regularly in consultation with the Finance Manager/Financial Policy & Development (FM/FPD) for approval by the appropriate authority. A request may be declined if the fee that is applicable to the request has not been paid. It should also be noted that provision of personal data to the requester by fax or e-mail is not recommended because of the privacy nature of the personal data.

65. Any decision to refuse compliance with a data access request should be authorised by a directorate officer. The subject office should seek the authorisation accordingly.

66. The administrative procedures in dealing with data access requests are summarised at **Annex K.** Reference may also be made to "A Guide for Data Users - No.2" published at [http://www.pcpd.org.hk].

Data Correction Request

67. A data subject, or his/her relevant person, is entitled to request correction of the personal data after a copy of the personal data has been supplied to him/her following a data access request, if he/she considers that the data are inaccurate.

Handling Data Correction Request

68. If it is satisfied that personal data which are subject to a data correction request are inaccurate, necessary correction has to be made and the data subject has to be supplied with a copy of the corrected personal data within 40 calendar days of receiving the request. If such cannot be complied with within the 40 calendar days reply period, the data subject should be informed of the reasons. The data correction request should then be complied with as soon as reasonably practicable.

69. If the personal data of a data correction request have been disclosed to a third party during the past 12 months before the day of correction of the data and there are no reasons to believe that such a third party has ceased using those data, the Department should supply such a third party with a copy of the corrected personal data and a written notice of the reasons for the correction. This requirement does not apply where the third party has obtained the data concerned by inspection of a public register without receipt of a certified copy.

70. A data correction request shall be refused under any of the following circumstances:

(a) insufficient information is provided to identify the data subject/relevant person; or

(b) it is not satisfied that the relevant person is properly authorised to seek correction.

71. A data correction request may be refused under any of the following circumstances:

(a) the request is not in writing in Chinese or English;

(b) it is not satisfied that the personal data are inaccurate;

(c) insufficient information is provided to ascertain that the personal data are inaccurate;

(d) it is not satisfied that the correction provided in the request is accurate;

(e) any other data user controls the processing of the personal data concerned in such a way that prohibits the compliance with the request; or

(f) a data correction request involves the correction of the personal data which is an expression of opinion or an unverifiable fact and it is not satisfied that the opinion or unverifiable fact is inaccurate.

72. If a data correction request is refused, the data subject should be informed in writing of the reasons of the refusal within 40 calendar days of receiving the request.

73. If a data correction request is refused under paragraph 71(e) above, the notice of refusal must include the name and address of the other data user concerned.

74. If a data correction request is refused under paragraph 71(f) above, a note of the data subject's proposed correction should be made and annexed to the data concerned in such a way that it is drawn to the attention of, or made available for inspection by, any person (including the Department itself or a third party) who may use such data in future. A copy of the note should also be attached to the notice of refusal to the data subject.

75. Any decision to refuse a data correction request should be authorised by a directorate officer.

76. The administrative procedures in dealing with data correction requests are summarised at **Annex L.**

Record of Refusals for Data Access and Correction Requests

77. A log book should be kept and maintained to record any refusals to comply with data access and correction requests and the reasons for refusals. The log book must be kept in Chinese or English. The particulars in the log book must be kept for a minimum period of 4 years.

78. The refusals shall be entered in the log book on or before the notice under paragraph 63 or 72 is served.

79. A sample format of the log book is at **Annex M**. If the Privacy Commissioner subsequently approves or issues such codes of practice to specify the format of the log book, such specified format should be followed.

80. The Privacy Commissioner or his authorised representative should be allowed to inspect and copy the log book at any reasonable time and without charge.

V. OUTSOURCING PERSONAL DATA PROCESSING

Obligations of data users

81. If a data user engages a data processor[3], whether within or outside Hong Kong, to process personal data on the data user's behalf, the data user must adopt contractual or other means to:

(a) prevent any personal data transferred to the data processor from being kept longer than is necessary for processing of the data; and

(b) prevent unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing.

82. Data users should make reference to the Information Leaflet on "Outsourcing the Processing of Personal Data to Data Processors" which was published by the Privacy Commissioner and can be downloaded at [http://www.pcpd.org.hk] under "*publications and videos*".

3 The term "data processor" is defined to mean "a person who (a) processes personal data on behalf of another person; and (b) does not process the data for any of the person's own purposes". With the wide meaning of the term, the scope of coverage of data processor is not limited to providers of IT processing. It also includes other contractors engaged to process personal data on behalf of the data user.

VI. EXEMPTIONS

Exemptions

83. Some types of personal data are exempt from certain requirements of the Ordinance under certain, specified circumstances. The exemptions are summarised at **Annex E**. There are some exemptions which may be more relevant to HA's general operation. They provide exemption from data access requirements or from restriction on use requirements as follows:

(a) exemption from the data access requirements - [S.53] on employment - staff planning, [S.55] on relevant process, [S.56] on personal references, [S.60] on legal professional privilege, [S.60A] on self incrimination;

(b) exemption from the restriction on use requirements - [S.60B] on legal proceedings, [S.62] on statistics and research, and [S.63C] on emergency situations;

(c) exemptions from the data access requirements and the restriction on use requirements - [S.57] on security, etc in respect of Hong Kong, [S.58] on crime, etc, [S.59] on health, and [S.61] on news.

84. It is important to note that the exemptions are limited in scope and some exemptions are subject to certain conditions or are of limited duration. Data users have the discretion to decide whether to make use of an applicable exemption in relation to any personal data which they hold. If data users have any doubt about the applicability of any exemption, legal advice should be sought.

85. Access to **employment-related personal data** should be granted subject to the applicable exemptions provided in the Ordinance. Besides, the guidelines in CSB Circular No. 13/2002 and any prevailing guidelines issued by Civil Service Bureau in respect of the applicable exemptions should be adopted.

VII. INTERFACE WITH THE CODE ON ACCESS TO INFORMATION

Code on Access to Information

86. Since 1996, the Department has been subject to the Code on Access to Information (the Code) by which members of the public should be given access to information on request, unless there is applicable exemption under the Code. When a request is made under the Code, the relevant requirements under the Code shall be complied with, and if personal data are involved, provisions of the Ordinance should also be followed.

Personal Data of A Deceased

87. Under the Code, personal data of a deceased may be disclosed to "Other Appropriate Person" meaning the closest living adult relative, executor or administrator of the deceased person's estate. Although the personal data relating to the deceased are outside the purview of the Ordinance, it is considered a good practice to follow the principles of the Ordinance in relation to data accuracy, retention, security etc. when handling the personal data of a deceased person. If the records concerned contain data of another identifiable living individual, the disclosure of his personal data would be subject to the requirements of the Ordinance.

Release of Information of Members of Advisory and Statutory Bodies

88. The following information of members of advisory and statutory bodies (e.g. the HA and its committees) amounts to personal data of the members and its disclosure is regulated under the Ordinance:

(a) attendance records;
(b) years of service on the particular body;
(c) occupation/profession by broad categories (e.g.

doctors, lawyers and company directors); and

(d) membership of other advisory and statutory bodies.

Although the Ordinance does not require the release of the information of the individual members of advisory and statutory bodies referred to above, the Code does. Under the Code, a department should entertain a request for information unless to do so would be harmful to the public interest.

89. Given the nature of the information in question and in the interests of transparency, the Committees' Section should inform HA Members (both existing and newly appointed) when collecting the information that the Secretariat will keep relevant records of individual Members as referred to (a) to (d) of paragraph 88 and that the records will be disclosed to the public upon request. As the purpose of keeping such records is to release them to the public, it is not necessary to obtain the Members' consent prior to the release. It would however be a good practice to inform them of the disclosure as soon as practicable in order to avoid them being caught by surprise when reporters approach them for comments.

90. All data users should also note that minutes of meeting attributing views to individual members of advisory and statutory bodies will amount to personal data of the members concerned. As these minutes (such as minutes of HA open meetings) may be released to the public upon request, the data users must take all practicable steps to explicitly inform the members concerned, before recording their views, that the minutes may be released to the public. Unless the members have been so informed, their voluntary and express consents are required for the release.

91. The arrangements mentioned in paragraph 89 are applied to requests for information referred to (a) to (d) of paragraph 88. If data users receive any request for other information relating to members of advisory and statutory bodies, they should consider the requests having regard to the Ordinance and the Code.