8 November 2002

Circular Letter: SU/CTR/2002/005

To: All Approved Trustees of Registered Schemes

Dear Sirs,

Outsourcing of Data Processing Functions to Places outside the HKSAR

It has come to our attention that there may be an increasing trend for MPF approved trustees to outsource part of the data processing functions, such as data input and document imaging, to service providers outside the HKSAR. The service provider may be an independent third party or more commonly an overseas branch or the parent/ affiliated company of the trustee ("overseas service provider").

Pursuant to Condition 4 of the Schedule of Conditions for Approval as a Trustee, a trustee is required to notify the Authority of any material changes occurring in respect of the information provided in its application for approval. An outsourcing arrangement to an overseas service provider is considered by the Authority as a material change and the trustee should notify the Authority of such arrangements.

For trustees who have already outsourced data processing functions to an overseas service provider, please submit the following information on the outsourcing arrangement, including the (1) functions, (2) commencement date, (3) name of the service provider, (4) place and jurisdiction under which the outsourcing is taking place and (5) a copy of the service agreement, if applicable, by **25 November 2002**. For trustees who are considering to outsource part of the data processing functions in the future, please submit the same to the Authority at the planning stage. To facilitate the Authority in assessing the capability of the overseas service provider in performing the delegated functions and the adequacy of internal controls, the Authority may request additional information/ documentation and may arrange an on-site visit to the overseas service provider in due course.

For all outsourcing arrangements, please be reminded to ensure that the existing/

proposed arrangements comply with the Personal Data (Privacy) Ordinance (Cap.486) ("PDPO"), in particular the six data protection principles (please see attached). In the event that an overseas service provider is being engaged, the trustee should ensure by contract or otherwise that the overseas service provider will comply with the relevant requirements of the PDPO in handling any personal data. In particular, the service provider should be required to pay due attention to the security of the personal data in its possession, refrain from using such data for any purpose other than for providing the service in the instructed manner, and either destroy the data or return them to the trustee once the service has been provided.

Should you have any questions, please do not hesitate to contact your case officer in the Authority. If you have any questions on the data protection principles or the requirements of the PDPO, please contact the Office of the Privacy Commissioner for Personal Data for assistance.

Yours faithfully,

(Peter Tsang)
Head
Supervision Division

Section of Enactment

Chapter:	486	Title:	PERSONAL DATA (PRIVACY) ORDINANCE	Gazette Number:	
Schedule:	1	Heading:	**DATA PROTECTION PRINCIPLES**	Version Date:	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)