

**Employment Service Support And Financial Assistance
Provided To Adult Rehabilitated Offenders**

**Administration's Response to
Issues raised at the meeting on 8 July 2003**

Removing the requirement of disclosing criminal records from the Government post application form

After consultation with departments, the Government agreed to delete the question on criminal convictions in the application form for government posts (G.F. 340). The Society for Community Organisation (SOCO) and government departments have been informed of the decision on 3 October 2003 accordingly. Amendment will be made to the application form as soon as possible. In the meantime, we will notify applicants for government posts that they are no longer required to answer the above question in the application form.

2. The Government has all along set a high standard of integrity for civil servants. As part of the recruitment procedures, the recruiting department/grade will arrange integrity checking for candidates whom they initially consider to be suitable for appointment. This is to ensure that the candidates are of good character and high integrity before they are offered appointment to the civil service. The recruiting department/grade will take into account the outcome of the integrity checking, the job nature of the post under recruitment and the department's operational requirements in determining whether an applicant is suitable for appointment. We will maintain the integrity checking system as it is conducive to public confidence in the civil service.

Employment quota in the civil service for rehabilitated offenders

3. The Government is an employer providing equal employment opportunities. Candidates are selected based on their ability, potential and performance, as well as the qualifications, experience and level of integrity required for the post under recruitment. The most suitable candidate will be selected. All applicants, irrespective of whether they are rehabilitated offenders or not, are subject to the same set of open and fair selection procedures. We consider it not necessary and indeed not appropriate to set an employment quota for rehabilitated offenders.

Information on the number of rehabilitated offenders employed in the civil service

4. We have not kept a central register on the number of rehabilitated offenders employed in the civil service. We consider that once an applicant is considered suitable in all aspects for and offered appointment to a post in the civil service, no distinction should be made as to whether he/she is a rehabilitated offender. Apart from protecting his/her privacy, this approach can ensure that he/she will receive fair treatment. If departments are to collect information on the number of

rehabilitated offenders currently working in their departments, they have to collect information previously provided by the officers in their application forms. During the process, the officers' past criminal records will be unnecessarily disclosed at the departmental level, which is considered inappropriate.

Response to the outstanding issues raised by the Society of Rehabilitation And Crime Prevention, Hong Kong (SRACP) and SOCO

5. The Government received the latest submissions from SRACP and SOCO on 4 July 2003 and 8 July 2003 respectively. Therefore, we were not able to address their latest recommendations in the information paper submitted to the Panel of Security on 26 June 2003. Our response to these issues are set out in the following paragraphs.

SOCO: to provide guidelines for the prevention of invasion of privacy by the Administration and other organizations

6. The Office of the Privacy Commissioner for Personal Data issued the Code of Practice on Human Resource Management (the CoP) in September 2000. It is clearly set out in Paragraph 2.7 of the CoP (see Annex 1) that in the process of seeking information about a job applicant for selection assessment, an employer should not collect personal data that are excessive in relation to the purpose. The paragraph provides practical guidance in respect of the requirement of Data Protection Principle 1(1)(c) specified in the Personal Data (Privacy) Ordinance (see Annex 2). The CoP is applicable to all data users including government departments and other organizations.

SOCO: to allow rehabilitated offenders to apply for Security Personnel Permits (SPPs) two years after release

7. The criteria for issuing SPPs are specified by the Security and Guarding Services Industry Authority (the Authority) under the Security and Guarding Services Ordinance, with the Commissioner of Police (CP) as the issuing authority. According to the original criteria for issuing a permit, no person who was convicted of a criminal offence would normally be granted a permit if he was within two years of release from a term of imprisonment, or was currently on probation or bound over.

8. Since security personnel are relied upon to discharge the important functions of safeguarding lives and properties of others, and there are chances for them to access sensitive information of their clients in performing their duties, the Authority considers that all security personnel should be persons well trusted by others. In view of their job nature, security personnel should have a high level of integrity and good character, the standard of which may be higher as compared with other jobs.

9. In a review on the policy governing the issuance of SPPs in 2001, the Authority noted that the original policy was not sufficient to debar unsuitable persons from entering the security industry. Therefore, the Authority recommended to tighten the “Good Character” criterion and conducted a 3-month consultation. The outcome of the consultation showed that about 71% of the respondents supported the tightening of the criterion. According to the recommendation of the Authority, it should be stipulated clearly that no person would normally be granted a permit if he had been convicted of specified offences including offences involving violence, fraud or dishonesty and sexual offences or had committed a number of offences within five years before submitting his application, or was within three years of release from a term of imprisonment. However, the CP could refer the application to the Authority for consideration if he is satisfied that the applicant is suitable for joining the security industry after considering the nature of criminal offence(s) committed by him/her.

10. When the Authority proposed to tighten the “Good Character” criterion, it also bore in mind the need to assist rehabilitated offenders. The Authority considered the proposed amendments struck a right balance between providing reasonable rehabilitation opportunities for offenders and rendering adequate protection for the public at large. The amended criterion was approved by the Legislative Council on 19 February 2003 and came into effect on 1 April 2003.

SRACP: to recognise SRACP as a training body offering specific training courses to rehabilitated offenders

11. Currently, the Employees Retraining Board (ERB) offers retraining courses to the public through some 130 training centres of over 50 accredited training bodies. These training bodies also provide placement services, job referrals and follow-up services to the trainees.

12. For better utilisation of resources, any persons may enroll in the placement-tied courses organised by the ERB if they are:

- (i) eligible employees in Hong Kong (such as Hong Kong permanent residents, new arrivals, etc.);
- (ii) persons aged 30 or above (as a major target group);
- (iii) at junior secondary level or below; and
- (iv) unemployed.

Any persons who meet the above basic requirements may enroll in any courses as appropriate. Applicants will not be classified as persons with/without criminal records.

13. The SRACP has previously applied for accreditation as a training body. However, its application was not supported by the ERB (Course Vetting Sub-committee) for the following reasons:

- (i) rehabilitated offenders may enroll in the various retraining courses offered by the training bodies approved by the ERB to facilitate their integration into society;
- (ii) it is not necessary to offer specific retraining courses to rehabilitated offenders as there is already a wide range of resources available to them and the ERB's retraining courses are comprehensive enough; and
- (iii) the employment services provided by SRACP are mainly on supportive basis with specific target employers. Apart from the potential labeling effect on the retrainee graduates, this is also different from the services provided by the ERB's training bodies which are open to all employers.

SRACP: to set up a working group on employment of rehabilitated offenders

14. A detailed account of the employment service support currently provided to rehabilitated offenders by the Government and the non-governmental organisations (NGOs) concerned is contained in the information paper (LC Paper No. CB(2)2677/02-03(06)) submitted to the Legislative Council Panel on Security on 26 June 2003. Immediately before the release of a prisoner, the Correctional Services Department assesses his/her case and refers it to the Social Welfare Department (SWD) and NGOs for follow-up actions if necessary. Publicity campaigns are also launched to appeal to the public and employers to accept rehabilitated offenders. In addition, the SWD provides support services to the vulnerable members of the community through close co-operation with the NGOs in its network of service. Presently, a wide range of services is already in place to assist rehabilitated offenders in employment and reintegration into society (please see LC Paper Nos. CB(2)2677/02-03(06) and also CB(2)2497/01-02(04) for details). It is considered unnecessary to set up a working group on the employment of rehabilitated offenders.

Security Bureau
November 2003

Extract from Code of Practice on Human Resource Management

As a matter of good practice, databases comprising personal data of job applicants should be accessible only to authorised staff using secure passwords on a "need-to-know" basis. Hard copy data should be located in secure areas. Personal data relating to job applicants stored on physical media such as paper or microfilm should be stored in locked cabinets in a secure room. In the event of such information being analysed or reviewed, the contents of that data should not be left unattended by, or out of the control of, authorised persons.

- 2.6.2 An employer should take all practicable steps to ensure that staff authorised to access personal data have the appropriate qualities of integrity, prudence and competence.¹

For example, an employer may implement training programmes to ensure that staff members who have responsibility for recruitment-related matters are made aware of the employer's personal data handling policy and practices, and carry out supervisory checks to ensure compliance with policy requirements.

2.7 Seeking Information for Selection Assessment

- 2.7.1 An employer may compile information about a job applicant, to supplement other data collected at the time of the original application, to assess the suitability of potential candidates for the job provided that it does not in the process collect personal data that are excessive in relation to the purpose.²

Generally, it would not be excessive to collect data to increase an employer's knowledge of a candidate's skills, good character, competencies or abilities, provided this knowledge were relevant in relation to the nature of the job. A common selection technique is by means of a selection interview or by requiring applicants to undertake a written skill test. Depending on the nature of the job, other selection techniques may involve an applicant in psychological tests, security vetting or integrity checking procedures. These selection techniques often entail collection of additional personal data from applicants.

For example, an employer may use a security vetting procedure to establish the security credentials of a potential candidate for a security guard's position if such knowledge is crucial prior to the employer's consideration to offer the job to the candidate. However, recording the details of a candidate's outside activities and interests might be excessive unless the employer can demonstrate that such detail is relevant to the inherent requirements of the job.

Integrity checking is usually concerned with ensuring the transparency and accountability of the post in respect of the capacity to which the potential candidate is appointed. However, the employer must be able to demonstrate that the collection of personal data, such as the candidate's investments or other financial matters, are relevant items essential for assessing the integrity of the individual concerned.

¹ DPP4(d)

² DPP1(1)(c)

- 2.7.2 An employer who compiles information about a job applicant pursuant to paragraph 2.7.1 should ensure that the selection method so employed does not involve the collection of personal data by means that are unfair.¹

As a matter of good practice, an employer should inform a job applicant before the selection method is used of its relevance to the selection process and the personal data to be collected by the chosen method.

2.8 Seeking Personal References of Job Applicants

- 2.8.1 An employer who wishes to obtain references from a potential candidate's current or former employers or other sources should ensure that such references are provided with the consent of the candidate concerned.

The PD(P)O requires the candidate's current or former employers to have the candidate's consent in providing references. Such consent may be given orally or in writing. As a matter of good practice, the prospective employer should consider seeking consent from the candidate prior to approaching the candidate's current or past employers or other sources for a reference. If this is the case, the prospective employer should, when requesting the reference, notify the source that provides the reference that consent has been given. If in doubt, the current or past employer should seek evidence of such consent from the requesting party, or verify this with the candidate.

2.9 Acceptance by Candidates

- 2.9.1 An employer may, no earlier than at the time of making a conditional offer of employment to a selected candidate, collect personal data concerning the health condition of the candidate by means of a pre-employment medical examination, provided that:

- 2.9.1.1 the personal data directly relate to the inherent requirements of the job;
- 2.9.1.2 the employment is conditional upon the fulfilment of the medical examination; and
- 2.9.1.3 the personal data are collected by means that are fair in the circumstances² and are not excessive³ in relation to this purpose.

For example, an employer may have a policy requiring a suitable candidate to undertake a pre-employment medical check by a nominated medical board to confirm whether the candidate is fit for employment. In this circumstance, the employer needs only to be provided with the minimum information about the candidate's health condition that supports the medical practitioner's opinion that he or she is fit for employment. Details of the candidate's medical history and treatment might be relevant for the medical board when conducting the medical check with the candidate, but these details need not be collected by the employer.

¹ DPP1(2)

² DPP1(2)

³ DPP1(1)(c)

雙語法例資料系統
Bilingual Laws Information System

[English](#)[繁體](#)[簡體](#)[繁體](#)[Gif](#)[簡體](#)[Gif](#)[Previous section of
enactment](#)[Next section of enactment](#)[Switch language](#)[Back to the List of
Laws](#)

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)

[Previous section of
enactment](#)

[Next section of enactment](#)

[Switch language](#)

[Back to the List of
Laws](#)