Information paper on
28 October 2002

Bills Committee on
Registration of Persons (Amendment) Bill 2001

Provision of Registration of Persons Records

INTRODUCTION

At the Bills Committee meeting held on 4 October 2002, Members enquired about the provision of Registration of Persons (ROP) data to other government departments under the existing legislation. A Member further enquired if any measure of control was in place to ensure that the ROP data would not be used by the Police for purposes other than those stated in their original request. This paper provides the relevant information.

EXISTING PRACTICE

2. Immigration Department (ImmD) deals with requests for provision of ROP data in accordance with the ROP Regulations. Under Regulation 24, ROP data shall not be disclosed except and unless with the written permission of the Chief Secretary for Administration. This authority has been delegated to the Secretary for Security. In processing such requests, both the Security Bureau and the ImmD observe the provisions of the Personal Data (Privacy) Ordinance (PD(P)O) on the use and disclosure of personal data.

3. Under the existing practice, any request for provision of ROP data must be made and signed by an authorized officer of appropriate rank, such as a Superintendent or above of the Police or an officer at the Assistant Director level of other government departments. The officer who authorizes the request must be satisfied that the personal data to be requested is for a lawful purpose directly related to a function or activity of his department, that the collection of data is necessary, and that the data

requested are adequate but not excessive. If the data subject has not voluntarily given his express consent to the use of his personal data, the relevant exemption provision in the PD(P)O must be specified and full justifications for the request must be given.

4. When the request is received by ImmD, an officer responsible for handling record check requests will check whether the purpose for which the request is made is the same as, or directly related to, any of the purposes for which the personal data were to be used at the time of collection and whether the consent of the data subject has been obtained. If not, he will check if the request is covered by any of the exemption provisions in the PD(P)O. Finally, he will ensure that CS's permission has been obtained for the data to be used for the purpose stated in the requesting memo. In case of doubt, the advice of the Department of Justice and the Privacy Commissioner for Personal Data will be sought as appropriate.

5. If the request is found to be lawful and a decision is taken to release the ROP data, ImmD will, when providing the data requested, specify that the data released should only be used for the purpose stated in the requesting memo, should not be shown to unauthorized persons, and should be destroyed when it is no longer required.

SPOT CHECK SYSTEMS ADOPTED BY IMMIGRATION DEPARTMENT

6. Spot check systems are adopted by ImmD internally and externally to ensure that all requests for provision of ROP data are handled in the proper manner and that the requests are indeed signed by the appropriate officers of other government departments. In the former case, instructions have been issued requiring the Unit Head and Section Head of the relevant records office to conduct spot checks at monthly and bi-monthly intervals respectively, with a view to ensuring that the approved policy and procedures are properly adhered to. In the latter case, the requesting departments will be asked by memo to verify some of the requests, chosen at random, to see if they are signed by authorized persons. For this purpose, the officer who verifies the requests must be at

least one rank higher than the one who signed the requesting memo. The spot check systems have been working effectively and no abuse has come to light so far.

MEASURES TAKEN BY THE POLICE TO PREVENT MISUSE OF THE ROP DATA

7. Police officers are required to follow clearly laid down procedures governing access to ROP data for investigation purpose. The procedures cover and provide adequate safeguards on the use, retention and disposal of ROP data. For example, there are clear restrictions regulating access to ROP data to ensure that the data is only made available to police officers on a "need to know" basis. Officers (normally the officer-in-charge of a case) requesting such data must apply to an approving/authorizing officer and fully justify to the latter's satisfaction that the request is for the purpose specified in the PD(P)O. The approving/authorizing officers are invariably senior police officers at the rank of Superintendent or above, and before approving/authorizing such applications and forwarding them to ImmD, they must satisfy themselves that the ROP data requested is necessary to assist the investigation.

8. Furthermore, all police officers have been instructed to take all practical steps to ensure that personal data held by a data user are protected against unauthorized access. ROP data which are no longer required for the purpose for which their collection is required will be destroyed.

Security Bureau
22 October 2002