

The Commissioner's power of inspection under the Personal Data (Privacy) Ordinance

I. The enabling provision : section 36

Section 36 of the Ordinance empowers the Commissioner to carry out an inspection on any **personal data system** used by a data user (e.g. Hospital Authority) or by a data user belonging to a class of data users.

2. The term “personal data system” is defined under section 2(1) to mean *“any system, whether or not automated, which is used, whether in whole or in part, by a data user for the collection, holding, processing or use of personal data, and includes any document and equipment forming part of the system”*.

3. The purpose of the exercise of the inspection power by the Commissioner is to assist him in making recommendations to the data user(s) relating to promotion of compliance with the provisions of the Ordinance, in particular, the data protection principles.

II. The legislative intent

4. The power of inspection was recommended in the Report of the Law Reform Commission on *Reform of the Law Relating to the Protection of Personal Data 1994*¹ to enable the Commissioner to initiate systematic on-site inspection of personal data system. The purpose of the power, as the Report suggests, *“would be to check that the data protection principles are being complied with and that appropriate control systems are in place. This should include verifying the accuracy of the organization's declaration and extend to a physical examination of the operational adequacy of such aspects as storage security... ”*.

5. When section 36 was examined at the Bills Committee stage, the Administration confirmed that it was based on the recommendation of the Law Reform Commission and clarified that the aim for carrying out an inspection was to provide *“...an overview on the personal data system used by a data user*

¹ See para 16.25 of the Report

so as to facilitate the Commissioner to make recommendations on how the system could be improved for promotion of compliance with the provision of [this Bill]. In the end, the data user concerned and his counterparts in the same sector would be benefited.”².

III. Inspection and compliance check distinguished

6. At present, the Commissioner carries out compliance checks from time to time when incidents of suspected privacy breach are brought to his attention without any complaint made by individuals affected.

7. The purpose of carrying out a compliance check is to gather, as soon as practicable, after the happening of the incident, first hand information and background materials which have led to the breach. This will enable the Commissioner to take prompt action as appropriate including, for example, the immediate cessation of any contravening act, the issuing of warning letters, the obtaining of an undertaking from the data user or the carrying out of a self-initiated investigation under section 38(b) of the Ordinance which may be followed by the issuance of an enforcement notice which the data user has to obey. This, however, is a reactive approach.

8. The power of inspection, on the other hand, is a proactive step taken by the Commissioner to conduct on-site privacy checks to “walk through the personal data system” used by the data user or the group of data users concerned. Prevention of data breaches is the common objective for carrying out an inspection. Upon completion of an inspection, the Commissioner shall inform the relevant data user of the result of the inspection and make recommendations to facilitate compliance with the Ordinance.

IV. The inspection power will be used for the first time

9. Since the establishment of the Office in 1996, the Commissioner has not exercised his inspection power under the Ordinance. It is due to lack of funds. Over the years, the Commissioner has not been provided with funds to carry out this particular function provided by law. His limited resources have

² See LegCo Paper No. HB 1308/94-95 on Notes of 9th Meeting.

to be applied in the handling of complaint cases and compliance checks arising out of reported privacy breaches.

10. The recent series of incidents on the loss of patients' personal data by various hospitals and clinics has caused the Commissioner serious concern. In view of the sensitivity of the personal data concerned, the number of patients involved as well as the huge volume of data lost, the Commissioner finds it compelling in the public interest to invoke this never before used power under the Ordinance to inspect the personal data systems in various hospitals managed by the Hospital Authority with a view to giving recommendations to facilitate its compliance with the Ordinance. The exercise of his inspection power is in addition to and does not affect the carrying out of the ongoing self-initiated investigations arising out of various incidents and the other investigation initiated by the patient affected.

V. The way forward

11. Inspection is of particular value in relation to the following aspects:-

- (i) increasing the data user's privacy awareness on self regulation;
- (ii) enhancing the supervisory and promotion function of the Commissioner; and
- (iii) applying the "prevention is better than cure" concept which is particularly useful in implementing adequate security measures to safeguard personal data from online leakage.

12. While the exercise of the power by the Commissioner has been hindered by resource constraints, the Commissioner strives to invoke this power as far as the limited resources permit to tackle the privacy risks posed by modern technologies and as effective control measures. The Commissioner appeals for more funding from the Government so that more inspections can be carried out.

-- END --