HONG KONG LAUNCHES DATA PROTECTION GUIDELINES

FOR PUBLIC & PRIVATE SECTORS

The Hong Kong government's data protection guidelines (see page 7) are the first in Asia to be addressed to computer users in general, and not be restricted to the finance sector, like those in Japan (see page 8). They follow the UK Data Protection Act in several respects, for example, in being limited to automated data, and excluding data indicating the intentions of the data user regarding the data subject. This summary highlights the main features of these guidelines:

Background

The guidelines are based on the Council of Europe Convention's data protection principles which were used by the Hong Kong governnment in its internal administrative guidelines published in September 1985. The principles in the new document are similar but follow more closely the "less legalistic wording" of the OECD Guidelines. The Hong Kong government's motivation for introducing the guidelines is that "Hong Kong's position as a financial and commercial centre could be jeopardized if there were restrictions imposed on the free flow of personal data to the territory from abroad." As a result, the government has accepted that data protection legislation should be enacted in Hong Kong. In the meantime, the government considers that "any immediate threat to the free flow of personal data to the territory...depend(s) as much on good data protection practice in Hong Kong as on the presence or otherwise of legislation."

Data Protection Principles

The data protection principles in the Hong Kong Guidelines are:

1. Openness - "a general policy of openness about developments, practices and policies"

2. Collection limitation - personal data collection "should be fair and lawful and, where appropriate, with the knowledge or consent of the data subject."

3. Purpose specification - "not later than at the time of data collection; subsequent use of personal data should be limited to the fulfillment of legitimate purposes already specified or such others as are not incompatible with them."

4. Relevance - "Personal data should be adequate, relevant and not excessive in relation to the purposes for which it is to be used."

5. Accuracy - "Personal data should be accurate and, where necessary, kept up to date."

6. Retention - "Personal data should not be kept for longer than is necessary for the purposes for which it is obtained."

7. Disclosure - "Personal data should not be disclosed for purposes other than those which have been specified except with the consent of the data subject or by the authority of law."

8. Subject access - "At reasonable intervals and without undue delay or expense, a person should be able to obtain confirmation of whether or not personal data is held (on him), to have communicated to him any such data in an intelligible form and, where appropriate, to have such data corrected or erased."

9. Security safeguards - "Personal data should be protected by appropriate safeguards against unauthorized access, alteration, disclosure or destruction and against accidental loss or destruction."

Responsibilties of Management

The Hong Kong Guidelines go beyond broad statements of principle to give operational guidance for organizations in any country and so the guidelines are given here in some detail:

1. Appoint a senior officer or committee to assess, authorize, monitor and review....personal data protection measures in existing and new computer applications.

2. Keep a record of relevant information about computer applications which store and process personal data, for example,

(a) the purposes of the applications;

(b) the types of personal data held;

(c) the kinds of persons on whom data is held;

(d) details of correlation of data obtained from different sources;

(e) the volume of data held; and

(f) those to whom data may be disclosed.

The data should be kept up to date at all times, registering significant changes to the type of information held as and when such changes occur."

3. "Effective compliance with the data protection principles requires active support from well-informed and well-motivated personnel....adequately trained in procedures to promote data protection."

For example, "adopt and distribute to all personnel concerned a clear statement of the organization's personal data protection policy."

4. "Collecting only the minimum amount of personal data that is essential for the intended purposes will minimize the risk of any improper use or disclosure of personal data. Data collected therefore should be restricted to that which is relevant and necessary to fulfill the intended purposes."

For example, "Personal data should be collected to the greatest extent practicable directly from the data subject."

5. "All personal data should be kept for the minimum period of time required to fulfill the purposes intended, after which the data should be erased."

Questions which might be asked during a review to determine whether data is still relevant and necessary are, for example, "When is it likely that the data will have fulfilled the purposes for which it was collected?"

6. "Reasonable validation of data held should be undertaken to ensure that the interests of the data subject are not harmed in any way by use of inaccurate, incomplete, irrelevant or out-of-date data."

For example, "contacts or correspondence initiated either by the data-using organization or by the data subject in the normal conduct of business could be used to confirm data accuracy."

7. "Within an organization, access to or disclosure of personal data should be on a "need to know" basis.

All requests for access to or disclosure of personal data should be carefully considered in the light of the data protection principles, for example, "that they are compatible with the purposes for which the data is collected."

8. "Full compliance at present with the subject access principle is not expected. The principle should be kept in mind however; indeed it would be prudent for the possibility of its future strict application (other than in clearly defined circumstances provided for by legislation e.g. national security) to be provided for when designing or purchasing new systems. It would certainly be good practice if measures providing for observance of the principle were to be devised and implemented in advance of any legal requirement."

(Editorial note. The management guidance on subject access, a key component of data protection laws everywhere, is less firmly stated than that on the other principles, and is quoted here in full so that readers can assess the text for themselves).

9. "Security measures should be implemented to guard against unauthorized access to and alteration, disclosure and destruction of personal data and against accidental loss or destruction of personal data held."

For example, "Procedures to guard against unauthorised access to computer files, passwords, audit trails, file access codes, etc."

Copies of the Hong Kong government's letter and guidelines are available from PL&B.