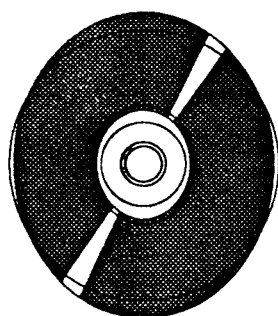


Sub-Committee on Technology & Law

Working Paper No. 1

# Data Protection in Singapore

*A Case for Legislation*



Law Reform Committee,  
Singapore Academy of Law

**Sub-Committee for Technology & Law**  
**SUMMARY OF WORKING PAPER 1**  
**DATA PROTECTION IN SINGAPORE**

1. The Working Paper is organised as follows:

SUBJECT	PARAS.	PAGES
1. Introduction	1-6	1-2
2. Reasons for Legislation	7-12	2-4
3. Basic Ideas	13-17	4-6
4. Present Legal Framework	18-26	6-8
5. Overseas Experience	27-57	9-16
6. Options for Singapore	58-98	17-26

2. The Sub-Committee decided that three subjects in the area of information technology merited attention: data protection, computer misuse and computer output as evidence. A statutory framework should provide for all three subjects. Data protection laws are intended to safeguard the rights of data subjects from abuse by those who use data in an unauthorised manner. With the growth in networking and the setting up of automated information systems, there is a very real danger of data users misusing personal information kept in the databases. A data protection law complements laws on computer misuse. (paras. 1-5)

3. The reasons for legislation are as follows:

- (a) Protection of data subjects' interests;
- (b) Provision of legal standards for data users;
- (c) Conformity with international instruments.

The protection of personal data is an aspect of protecting individual privacy. Such protection can also benefit data users as it ensures that data kept by them is up-to-date and accurate. The second reason for legislation is that there should be legal professional standards set for data users. Existing law is

inadequate and is not preventative in nature. Thirdly, international conventions may allow countries adhering to them to impose restrictions on transborder data flows to countries which do not have such legislation. This may be damaging to the long-term interests of Singapore which aim to be a "global city" as well as an "information resource centre." (*paras 7-12*)

4. In **Basic Ideas**, the idea of "data protection" was distinguished from other related concepts such as Privacy and Freedom of Information. Data protection concerns not just the interests of individual data subjects but also attempts to balance the interests of data users as well. Personal information or data is also another vital concept. Here care must be taken to distinguish data concerning natural persons from legal persons. There is no real need to cover corporations in data protection legislation and to include them may be impractical. (*paras 13-17*)

5. In the review of existing law, it was shown that although some legislative provisions could be regarded as part of data protection law, these were mainly in the public sector and were not computer-specific. In terms of the private sector, the main recourse is to the civil law remedies. These are founded in contract and tort and are not particularly suited for use in the area of data protection. (*paras 18-26*)

6. The **International Legal Instruments** were next examined (*paras. 27-45*). These provide the guidelines which have determine almost all national legislation in overseas countries and which may also be applicable here. The international instruments provide for general principles concerning the information cycle, namely, collection, processing, use and disclosure of data. The Principles in general are meant as minimum standards for any legislation.

7. The **Principles** include: lawful and fair collection of data, quality of data, purpose specification in collection, use of data only for specified purposes, proper security, rights of access by data subjects to such information.

8. **National legislation** however varied widely in scope. Some countries legislate to control only the public sector. At the other end, there are countries which include manual files as well as automated data files. They also include

information about "legal persons" within their ambit. The more important features of such legislation are that they normally have general principles followed by enforcement machinery to ensure that the rights of access given to data subjects are genuinely effective.

9. It is also important to note the competing interests of protecting certain interests in the public sector as well as in the private sector. Examples of these interests are: national security, prevention of crime and or preventing harm to the economy. The function of a data protection law should balance the interests of the individual with the broader social interests. The demands of individual privacy may have to give way to public interests. Certain exemptions from the obligations either of registration or of disclosure should be noted. These refer in the main to national security or other matters which may affect public order. Manual records are not included unless they are part of an automated information system. Certain records kept by individuals for their recreation or domestic use are usually not included. (*paras 46-57*)

## **PART II: OPTIONS**

10. The Sub-Committee recognises that data protection laws may introduce new rights to data subjects and this may be viewed in some quarters as unnecessary. However, it is felt that the long-term interests of the country would be better served by having such legislation, the only issues mainly being the nature of the legislation and the appropriate time for introducing it.

11. In discussing the nature of the legislation, the Sub-Committee looked at the following options:

- (i) No further legislative action necessary as existing law is sufficient;
- (ii) Voluntary codes of conduct unsupported by legislation;
- (iii) Legislation in the public but not the private sector;
- (iv) Legislation in the private but not the public sector;
- (v) Legislation for all sectors.

The arguments for and against each option may be found at paragraphs 61-67. Other issues discussed are whether only automated information systems ought to be controlled or whether they should include manual records as well. The relationship between primary and secondary legislation is also studied: it is noted that as technological change can be rapid, it may be expedient to provide

broad primary legislation and to effect closer control of each sector through secondary legislation. (*paras 68-75*)

12. In terms of content, the legislation may adopt "Principles" similar to those set by the OECD and the Council of Europe Convention but taking into account the new technologies of telemetry, interactive media and electronic mail as well.

13. "Personal information" may be looked at from the "sensitivity" point of view, objectively ascertained. The Sub-Committee felt that a scheme which did not differentiate between "sensitive" data and "non-sensitive" data would be difficult to justify and run. A scheme of registration of data users dealing with sensitive data may be more defensible. Data users with less sensitive or non-sensitive data may only need to give details of the types of information kept without being required to follow stringent rules controlling the use of sensitive information. (*paras 76-80*)

14. The Sub-Committee considered various options as to which institution is suitable to act as the data protection agency. The options are:

- (i) Attorney-General's Chambers;
- (ii) An appropriate Government Department;
- (iii) the National Computer Board;
- (iv) An autonomous institution.

Additionally, a Data Protection Appeals Board should be set up to hear appeals. The discussion is at paragraphs 81-88.

15. The Sub-Committee also discussed the issue of data-sharing. Data sharing should be a benefit of automated information systems. At the same time, the risk of abuse is enhanced as data supplied for one purpose may be unsuitable for another. The principles governing data sharing are discussed at paragraphs 89-94 of the main Paper.

16. In paragraphs 95 and 96, the Sub-Committee mentioned that the existing law providing the data subjects with remedies should be buttressed by statutory rights allowing access to data and correction or deletion of the same. Additionally, a statutory right to civil remedies or criminal proceedings should perhaps be enacted to provide an extra avenue of redress for the aggrieved data subject.

17. Finally, the Sub-Committee recognises that there should be exemptions either from registration of certain data users or disclosure of certain categories of information or data. Exempt institutions may include those dealing with national security or international affairs. Data excluded from disclosure may be

those relating to the prevention of crime or the preservation of public order.  
(paras 97-8)

***The Sub-Committee invites comments of interested parties on the matters  
discussed in the Working Paper.***

\*\*\*\*\*