DATA PROTECTION IN SINGAPORE

REGULATION

1. What national law(s) apply to the collection and use of personal data? If applicable, has Directive 46/1995/EC on data protection (Data Protection Directive) been implemented?

Personal Data Legal Landscape

The collection and use of personal data in Singapore are regulated to a certain extent by the common law, a multitude of statutory provisions that address the issue according to subject matter, various self-regulatory industry codes and the co-regulatory Model Data Protection Code (discussed below).

Mandatory Legislation

For example, sector-specific statutes such as the Banking Act, Official Secrets Act, Statistics Act and the Central Provident Fund Act, as well as subsidiary legislation like the Telecommunications Competition Code, contain legally mandatory provisions on the collection and use of personal data in various differing circumstances, while the Computer Misuse Act generally prohibits and criminalises unauthorised access to information on a computer system.

The above examples are by no means an exhaustive list of the numerous and disparate pieces of legislation in Singapore that touch upon the matter of personal data protection in some form or other. These typically regulate and criminalise the unauthorised release of personal information by the bodies and agencies that collect information about individuals, but do not generally accord rights to individuals to control the collection, use and dissemination of their personal information.

Self-Regulatory Industry Codes

In addition, various self-regulatory industry codes of practice such as the Singapore Code of Advertising Practice and the Code of Practice of the National Association of Travel Agents in Singapore also seek to address personal data protection, based on their respective industry-specific modes and structures of implementation and enforcement.

Co-Regulatory Model Data Protection Code

With respect to the general protection of personal data, the approach in Singapore is based on a co-regulatory one whereby the government's role is existent but limited and industry is encouraged to be involved in maintaining standards of personal data protection. This is done through a system in which organisations voluntarily wishing to be accredited as having met and complied with, *inter alia* but for the most part, prescribed standards of personal data protection and thereby being awarded the "TrustSg" status, may do so by adopting the prescribed code of conduct which includes the provisions of the Model Data Protection Code for the Private Sector.

The current revised version of the Model Data Protection Code for the Private Sector with its accompanying implementation and operational guidelines (collectively "the Code") was established and released in December 2002 by the National Trust Council ("NTC") which is an industry-led organisation supported by the government. The Code sets out the prescribed conduct for the protection of personal information and is organised around 10 basic Data Protection Principles, broadly differentiated according to the various stages of data processing. Once adopted by an accredited organisation, that organisation must adhere to all the Data Protection Principles in the Code and cannot do so selectively.

The NTC co-ordinates the use of the Code and evaluates and nominates companies to act as Authorised Code Owners, who are in turn responsible for evaluating and accrediting companies under the "TrustSg" accreditation scheme. Companies which are so accredited are entitled to display the "TrustSg" mark at their storefronts and websites.

The Code is modelled on the Canadian Standards Association's Model Code for the Protection of Personal Information ("CSA Code"), which is itself based on the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* established by the Organisation for Economic Cooperation and Development ("OECD Guidelines"). In the development of the Code, guidance was also taken from the EC Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data (95/46/EC) ("the EU Directive") but the EU Directive cannot be said to have been implemented as such in Singapore.

As the Code effectively sets out the prescribed standards of general personal data protection in Singapore, albeit on a voluntary accreditation basis, the answers to the rest of the questions below are based only on the Code and do not address the possibly disparate treatments under the other sector-specific legislation or industry-specific codes mentioned above.

2. To whom do the rules apply (EU: data controller)?

The Code is available for voluntary adoption by private sector consumer businesses such as retailers (including e-tailers), direct marketers, financial institutions, telecommunications companies, product manufacturers, service providers, etc.

The Data Protection Principles in the Code have been framed in general terms so that they may be adopted across sectors by a wide range of organisations and apply:

- to the organisation that collects, uses, manages and/or controls personal data, regardless of whether the data are transferred out of Singapore,
- for the benefit of all persons, whether or not resident in Singapore, whose data are or have been processed by that organisation.

3. What data is regulated (EU: personal data)?

The Code applies to the processing of personal data in electronic form, whether or not such processing takes place by electronic means.

Personal data is defined in the Code to mean:
"data, whether true or not, in an electronic form, which relate to a living person who can be identified —

- from those data; or
- from those data and other information which is in the possession of, or is likely to come into the possession of, the organisation."

Such personal data may include an individual's name, age, weight, height, National Registration Identity Card number, medical records, income, purchases and spending habits, race, ethnic origin and colour, blood type, DNA code, fingerprints, marital status and religion, education, home address and phone number.

In addition, personal data kept in non-electronic form and then subsequently converted into electronic form will also be subject to the Code from the point of conversion onwards, whereas, electronic data even if presented in non-electronic form (e.g. by being printed) will still be subject to the Code.

However, an organisation may additionally choose to subject the data it keeps or handles in non-electronic form, to the operation of the Code, on a voluntary basis.

4. What acts are regulated (EU: processing)?

The Code regulates the collection, processing, use, disclosure and retention of personal data.

5. What is the jurisdictional scope of the rules?

The Code applies to any personal data which is processed or controlled by the organisation in question, and as stated in the response to Question 2 above:

- regardless of whether the data are transferred out of Singapore; and
- in favour of all persons, whether resident in Singapore or not, whose data are or have been processed by that organisation.

6. What are the main exemptions (if any)?

The following data processing activities, where appropriate, may be exempted from the purview of the Code:

- processing required by any law or by the order of a court;
- processing by any person purely for that person's family, household or personal affairs (including recreational purposes);
- processing purely for journalistic, artistic or literary purposes;
- processing by any organisation directly relating to a current or former employment relationship between the organisation and the individual (although the organisation in question may opt to restrict this exemption only to such processing activities necessary for the purposes of carrying out its obligations under the employment relationship);
- any processing operations which are necessary to safeguard –
  - national and public security;
  - national defence;

- the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
- an important national economic or financial interest, including monetary, budgetary and taxation matters;
- monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority;
- the protection of the individual or of the fundamental liberties of others under the Constitution; and

- processing for research or statistical purposes, provided the results of the research or any resulting statistics are not made available in a form which identifies any individual.

7. Is notification or registration required before processing data? If so, please provide brief details.

The Code requires the processing organisation to:

- specify the purposes for which the personal data is collected at or before the time the data is collected, or if this is not practicable, as soon thereafter as is reasonable;
- ensure that the said purposes are stated in documented form and in such manner that the individual can reasonably understand why the data is being collected and how the personal data will be used or disclosed;
- obtain the consent and ensure the knowledge of the individual for the collection, use or disclosure of that individual's personal data, subject to certain permitted exceptions; and
- only collect, use and disclose such personal data as necessary for such purposes as shall have been specified by the organisation (in the manner stated above), subject to certain permitted exceptions.

MAIN DATA PROTECTION RULES AND PRINCIPLES

8. What are the main obligations imposed on data controllers to ensure that data is processed properly?

Under the Code, a data controller is obliged to ensure that:

- it is responsible for personal data in its possession or custody and for such purpose, shall –
  - designate a person or persons who will be accountable for the data controller's compliance with the Code and who must
    - establish and keep up-to-date policies and procedures to protect personal data;
    - prepare impact assessments of both current and proposed information systems on data protection;
    - ensure the implementation of the data controller's data protection policies and procedures by other organisations to which data processing functions are outsourced;
    - educate the data controller's employees on the importance of data protection; and

        - stay abreast of technical and legal developments in this field in order to enable the data controller to maintain the highest reasonable security standards; and
    - take reasonable steps to ensure that any data it transfers to someone will not be processed inconsistently with the Code
- the purposes for which the personal data are collected are specified by the data controller;
- the knowledge and consent of the individual are obtained for the collection, use or disclosure of that individual's personal data, subject to certain permitted exceptions;
- the collection of personal data shall be –
    - limited to that which is necessary for the purposes specified by the organisation, subject to certain permitted exceptions; and
    - by fair and lawful means;
- personal data shall –
    - not be used or disclosed to a third party for purposes other than those for which it was collected, unless the individual consents to such use or disclosure or certain permitted exceptions apply; and
    - subject to any applicable legal requirements, be retained only as long as necessary for the fulfilment of those purposes, in connection with which
        - the data controller should develop guidelines and implement procedures on the retention and destruction of personal data; and
        - where personal data have been used to make a decision about an individual, such personal data shall be retained long enough to allow the individual access to the data after the decision has been made;
- personal data shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used, taking into account the interests of the individual in question, so as to minimise the possibility that inappropriate data may be used to make a decision about the individual;
- personal data shall be protected by appropriate security safeguards;
- information about the data controller's policies and procedures for handling personal data shall be made readily available;
- an individual shall –
    - upon his request, be informed of the existence, use and disclosure of his personal data and be given access to that data, subject to certain permitted exceptions;
    - be able to challenge the accuracy and completeness of his personal data and have them amended as appropriate; and
    - be provided with the reasons for being denied the said access upon request;
- an individual shall be able to address a challenge concerning compliance with the Code to the designated person or persons accountable for the data controller's compliance, for which purpose –
    - mechanisms and processes, which are simple and accessible, shall be put in place to receive and address complaints or inquiries about the data controller's policies and procedures on the handling of personal data; and
    - all complaints shall be investigated and if found to be justified, the data controller shall take appropriate measures, including if necessary, amending its policies and procedures.

9. Is the consent of data subjects required before processing personal data? If so: What rules are there regarding the form and content of consent? Would online consent suffice? Are there any special rules regarding the giving of consent by minors?

Form and Content of Consent

The Code provides that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal data. However the Code does not specify the form or content of such consent. In particular, the Code states that:

- consent may be implied where the purpose for which data are collected is obvious and aligns so closely with the individual's expectations;
- consent does not have to be obtained by the organisation directly from the individual;
- the form of consent sought by the organisation may vary, depending upon the circumstances and the type of data collected, so that generally, express consent should be obtained for sensitive data while implied consent may suffice for less sensitive data;
- for example, an individual may give his consent –
  - by completing and signing an application form which provides information on the intended use of the data;
  - in a form which includes a check off box specifying his request not to provide his name and address to other organisations;
  - orally where data is collected over the telephone; or
  - with other opt-out measures which are fair and reasonable.

Consent by Minors

There are no such special rules enshrined in the Code on the giving of consent by minors, although the Code does make an incidental reference to the fact that seeking consent may be inappropriate when the individual is a minor.

This, however, does not alter the substantive law on contracting with minors and the possibility of obtaining the consent of the legal guardian of the minor in question.

10. If there is no consent, on what other grounds (if any) can processing be justified?

The Code expressly states the specific exceptional circumstances where personal data may be collected, used or disclosed to third parties without the knowledge or consent of the individual as follows.

Collection or use of the data without knowledge or consent of the individual (including such collection or use beyond the specified purposes for which the data are collected and hence without the effective knowledge or consent of the individual) is permitted where:

- the collection/use is clearly in the interest of the individual and it is impracticable to obtain the consent of the individual to that collection/use and if it were practicable to obtain such consent, the individual would be likely to give it;

- collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the data where such collection pertains to, or otherwise where data is used in, an investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being, or is about to be committed;
- data is being collected/used in an emergency that threatens the life, health or security of a person; or
- collection/use is of data which is generally available to the public.

Disclosure of the data to a third party without the knowledge or consent of the individual (including such disclosure beyond the specified purposes for which the data are collected and hence without the effective knowledge or consent of the individual) is permitted where the disclosure is:

- clearly in the interest of the individual and it is impracticable to obtain the consent of the individual to that disclosure and if it were practicable to obtain such consent, the individual would be likely to give it;
- made to a solicitor representing the organisation;
- necessary for the purposes of establishing, exercising or defending legal rights;
- made to a government agency that has made a lawful request for the data;
- made to a person who needs the data because of an emergency that threatens the life, health or security of a person;
- made to an institution whose purpose is the conservation of records of historic or archival importance and disclosure is for such purpose;
- of data which is generally available to the public in that form; or
- reasonable (and in the case of disclosure beyond the specified purposes of the collection of the data, made by an investigative body) for purposes related to the investigation of an actual or suspected breach of an agreement or contravention of the law that has been, is being or is about to be committed; or
- in the case of disclosure beyond the specified purposes of the collection of the data, is made on the initiative of the organisation, to an investigative body appointed by the organisation, or to a government agency for investigative purposes.

11. Do special rules apply in the case of certain types of personal data, for example sensitive data? If so, please provide brief details.

The Code acknowledges that certain data may be more sensitive than others and that accordingly such more sensitive data require a higher degree of protection. Hence:

- in requiring the organisation to protect personal data by appropriate safeguards, the Code provides that the nature and extent of such safeguards will vary depending on, *inter alia,* the sensitivity of the data; and
- the Code states that –
    - an organisation should generally seek the express consent of an individual when the data involved are likely to be considered sensitive, and
    - implied consent would generally be appropriate when the data are less sensitive.

The Code further clarifies that although certain data such as medical and income records are almost always considered to be sensitive data, any datum can in fact be considered as sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive data but the names and addresses of subscribers to some special-interest magazines may be considered sensitive.

RIGHTS OF INDIVIDUALS

12. What information should be provided to data subjects at the point of collection of the personal data?

The Code provides that at the point of collection of the personal data, the data subject should be informed of:

- the purposes for which the personal data are collected; and
- the organisation's policies and procedures for handling personal data.

13. What other specific rights (such as a right of access to personal data or the right to object to processing) are granted to data subjects?

Under the Code, a data subject has the right:

- to acquire information about the organisation's policies and procedures on the management of personal data, without unreasonable effort and in a form that is generally understandable;
- upon request (subject to the exceptions discussed below and possibly but not necessarily upon payment of a reasonable fee), to be informed of the existence, use and disclosure of his personal data within a reasonable time and in a form that is generally understandable, to be given access to that personal data and where such access is denied, to be informed of the reasons for being so denied;
- to be given the opportunity to challenge the accuracy and completeness of his personal data and have such data amended as appropriate;
- to address a challenge concerning compliance with the Code to the designated person or persons accountable for the organisation's compliance and –
    - where a data subject makes inquiries or lodges a complaint, to be informed of the existence of relevant complaint mechanisms; and
    - to have his complaint investigated.

However, a data subject's request for information on or access to his personal data *shall* be refused where:

- providing access would be likely to reveal personal data about another person, unless the said person consents to the access; or the data subject needs the information because a person’s life, health or security is threatened, provided that where the data about the said person is severable from the record containing the data about the individual, the organisation should sever the data about the said person and provide the individual access; or
- an investigative body or government agency, upon notice being given to it of the data subject's request, objects to the organisation complying with the

request in respect of its disclosures made to or by that investigative body or government agency.

Furthermore, the organisation *may* refuse the data subject's request for information on or access to his personal data where:

- the data is protected by solicitor-client privilege;
- it would reveal data that cannot be disclosed for public policy, legal, security, or commercial proprietary reasons, provided that where the personal data about the individual is severable from the record that cannot be disclosed for public policy, legal, security or commercial proprietary reasons, the organisation should sever the data and give the individual access;
- it would threaten the life, health or security of a person;
- the data was collected without the data subject's knowledge or consent because such knowledge or consent would compromise the availability or accuracy of the data and such collection pertained to an investigation of a breach of an agreement or the law;
- complying with the request would be prohibitively costly to the organisation; or
- the request is frivolous or vexatious.

SECURITY REQUIREMENTS

14. What security requirements are imposed in relation to personal data?

The Code provides that personal data must be protected by appropriate security safeguards, in particular, against accidental or unlawful loss, as well as unauthorised access, disclosure, copying, use, or modification and should protect personal data regardless of the format in which the data are held.

The nature and extent of the safeguards will vary depending on:

- the sensitivity of the data that have been collected;
- the amount, distribution, and format of the data;
- the method of storage;
- the state of technological development; and
- the cost and reasonableness of implementation of the safeguards.

Further, the methods of protection may include one or more of the following:

- physical measures, for example, secured filing cabinets and restricted access to offices;
- organisational measures, for example, security clearances and limiting access on a "need-to-know" basis whereby –
  - the employee who gains access should need to do so in the performance of his duties; and
  - access by the employee must be in support of a legitimate business function of the organisation;
- technological measures, for example, the use of passwords and encryption, as may be available, appropriate and reasonable from time to time.

The organisation is further required to:

- take reasonable care in the disposal or destruction of personal data, to prevent unauthorised parties from gaining access to the data; and
- verify the identity of the individual concerned before granting access to such individual who makes a request for access to his personal data.

PROCESSING BY THIRD PARTIES

15. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

The Code expressly provides that the designated person or persons of the data controller must ensure the implementation of the data controller's data protection policies and procedures by other organisations to which data processing functions are outsourced.

More generally and not necessarily only in relation a third party who processes data on behalf of the data controller, the Code also obliges the data controller to:

- take reasonable steps to ensure that data to be transferred will not be processed inconsistently with the provisions of the Code; and
- provide, upon request, information on the recipients or categories of recipients to whom it has disclosed personal data about an individual in as specific a manner as possible and where it is not possible to provide a list of the organisations to which it *has* actually disclosed such data, then to provide a list of the organisations to which it *may* have disclosed such data.

INTERNATIONAL TRANSFER OF DATA

16. What rules govern the transfer of data outside your jurisdiction?

The Code applies to:

- personal data which are processed or controlled by the organisation whether or not such data are transferred out of Singapore; and
- all persons whose data are processed by the organisation, whether or not such persons are resident in Singapore.

Where data are to be transferred to third parties, the organisation must take reasonable steps to ensure that such data will not be processed inconsistently with the provisions of the Code. Such a requirement applies whether or not the third party is located in Singapore so as to ensure that such personal data will receive similar levels of protection even when they are exported out of Singapore. This concept is based on the restrictions on international transfers of personal data contained in Article 25 of the EU Directive.

ENFORCEMENT AND SANCTIONS

17. What are the enforcement powers of the national regulator?

Given the nature of the scheme adopted for the implementation of the Code as discussed in the response to Question 1 above, the national regulator is not vested with enforcement powers as such in the sense of meting out sanctions or penalties to non-compliant organisations. Instead, the scheme operates on the basis whereby:

- aggrieved individuals are entitled to lodge complaints and challenge compliance of the Code directly with the organisation in question, who is obliged under the provisions of the Code, to investigate such complaints and take appropriate measures in response;
- where a complaint is not resolved, the aggrieved individual may seek the assistance of either of the (currently) two Authorised Code Owners appointed by NTC who are charged with accrediting the organisations who adopt the provisions of the Code and who may –
  - assist with resolution of the dispute through mediation services;
  - issue a warning to the organisation in question in the appropriate circumstances; or
  - ultimately withdraw the accreditation of the organisation which is found to be in breach of the Code.