Data protection in South Africa

This article was first published in De Rebus November 2005 issue

Introduction:

Whether you use the internet to network or trade, you are likely to be requested to provide some personal data at some point. Collection of personal data in electronic format is made easy by computers and cell phones alike, and vast volumes of data can easily be sent or stored for unlimited periods.

Consumers, however, are often not informed about their rights and possible consequences of rendering such personal information to data collectors. In this regard, collection and use of personal data may result in the invasion of an individual's privacy rights. Data may be disclosed or accessed without authorisation or used for a different reason for which it was collected.

Collecting data electronically also poses various risks for data collectors. In this regard, there may be risks that the data provided may be inaccurate, false, incomplete or irrelevant.

Data collection poses international legal challenges and many countries have adopted "data protection" laws. "Data protection" has a technical meaning and generally refers to the collection, storage, use and transmission of "personal information". It therefore does not apply to all types of data.

International developments:

In the 1980s, a number of international organisations, including the Organisation for Economic Co-operation and Development (OECD), the European Council and the European Economic Community started a process of exploring and developing means to conform data protection standards in every country to ensure the free flow of information cross-country borders. As a result two significant international documents were issued, namely the European Council's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the OECD's Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

In 1995 a further important document was issued by the European Union, namely Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such data (Directive 95/46/EC). Article 25 of this Directive prescribes that a member state must prohibit the transfer of personal data to non-member states that do not ensure adequate levels of data protection.

The development of these international instruments did not involve the United States of America as member state. The United States of America did not have any data protection laws which applied to all its states on a federal level. Different legislations and data protection levels apply and there is no provision for a central data protection authority. The EU countries did not initially find the USA personal information protection system adequate and a separate agreement was negotiated to ensure the free flow of personal data to and from the USA. This "Safe Harbor" agreement was adopted in 2000 and consists of a set of privacy principles. USA companies may voluntarily self-certify to comply with these principles and these principles are not mandatory for USA companies.

Developments in South Africa:

South Africa became a democracy in 1994. This development led to the development of the Bill of Rights (Chapter 2 of the Constitution of the Republic of South Africa) which expressly provides for the protection of the right to privacy of individuals. It was also South Africa's objective to develop national legislation which would ensure an adequate level of data protection to meet the requirements of the EU Directive.

The South African Law Reform Commission (SALRC) published a discussion paper (Green Paper) on the issue of privacy and data protection in October 2005. The discussion paper included a draft Bill on the Protection of Personal Information. A copy of this draft Bill can be downloaded at:
http://www.justice.gov.za/legislation/bills/B9-2009_ProtectionOfPersonalInformation.pdf

The proposed Act applies to personal information collected, stored and disseminated by automated and non-automated processes. It generally applies to South African businesses processing personal information in the context of their trade activities. The proposed Act will for instance not apply to the processing of personal information in the course of a purely personal or household activity. It further applies to the processing of personal information by/for businesses established outside South Africa using automated or non-automated means situated in South Africa. The proposed Act binds the State.

The Act will also establish a body known as the Information Protection Commission, of which the chairperson and two ordinary members will be appointed by the State President. The duties of the Commission will include education, monitoring compliance and dealing with complaints.
Chapter 3, Part A provides for the principles for the processing of personal information, which are in line with main principles set out in the EU Directive and includes in short the following:

- Principle 1: Processing limitation: Personal information must be processed in accordance with the law and in a proper and careful manner in order not to intrude upon the privacy of the data subject to an unreasonable extent.

- Principle 2: Purpose specific: Personal information must be collected for a specific, explicitly defined and legitimate purpose. Personal information may not be kept for longer than is necessary for archiving purposes.

- Principle 3: Further process limitation: Personal information must not be further processed in a way incompatible with a purpose for which it has been collected in the first instance.

- Principle 4: Information quality: The data collector collecting and processing personal information must take practical steps to ensure that the personal information is complete, not misleading, and accurate.

- Principle 5: Openness: Personal information may only be collected by a data collector which has give notice and has been recorded in a Register kept by the Commissioner.

- Principle 6: Security safeguards: Appropriate technical and organisational measures must be taken to secure the integrity of personal data by safeguarding against the risk of loss of, or damage or destruction of personal information and against the unauthorised or unlawful access to, or processing of personal information.

- Principle 7: Individual participation: Where personal information is collected, the data subject is entitled to obtain, free of charge, confirmation whether and what personal information is being kept.

- Principle 8: Accountability: The responsible party must ensure that there are measures taken that give effect to the Principles set out in Chapter 3, Part A.

Chapter 3, Part B deals with the prohibition on the processing of "special personal information". In this regard, in principle, it is prohibited to process personal information concerning a person's religion or philosophy of life, political persuasion, health or sexual life, or trade union membership, criminal behavior, or unlawful or objectionable conduct connected with a ban imposed with regard to such conduct, except where the data subject has given his/her explicit consent to the processing of the information. However, Part B further sets out various exemptions to this general prohibition on the processing of special personal information as described. For instance, the prohibition on processing of personal information relating to a person's health or sex life will not apply where the processing is carried out by medical professionals and it is necessary for proper treatment.

Chapter 4 provides for exemptions from the 8 information protection principles referred to above, and set out fully Chapter 3, Part A. In this regard, the Commission may authorise a responsible party (data collector) to process personal information, even though that processing would otherwise be in breach of an information protection principle, if the Commission is satisfied that, in the special circumstances of the case:

- the public interest in that processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from that processing; or
- that processing involves a clear benefit to the data subject or a third party that outweighs any interference with the privacy of the data subject or third party that could result from that processing.

Any person may submit a complaint to the Commission alleging that any action is, or appears to be, for instance, a breach of any information protection principle. A complaint may be made either orally or in writing. A complaint made orally must be put in writing as soon as reasonably practicable. The Commission must provide such reasonable assistance which is necessary in the circumstances to enable an individual who wishes to make a complaint to the Commission, to put the complaint in writing. It is the function of the Commission to then conduct investigations and decide whether to take formal action or not.

If the Commission is satisfied that a responsible party has interfered with the protection of the personal information of a person by, for instance, breaching the information protection principles, the Commissioner may serve a notice on the responsible party requiring the responsible party to refrain from proceeding with the processing of personal information within a specified period.

A data subject or the Commission may also institute civil court proceedings against any responsible party who has contravened the provision of the Act for *inter alia* payment of damages, interest and costs of suit.

Any person who hinders, obstructs or unduly influences the Commission or any person acting on behalf of, or under the direction of the Commission in the performance of the Commission's

duties and functions under this Act, will be guilty of an offence. Any person convicted of an offence may be imprisoned or fined or both.

Section 94 of the proposed Act further provides that a responsible party in South Africa may transfer personal information about a data subject to someone who is in a foreign country only if:

(a) The recipient of the information is subject to a law, binding scheme or contract which effectively upholds the fair handling of the information that is substantially similar to the information protection principles; or
(b) The data subject consents to the transfer; or
(c) The transfer is necessary for the performance of a contract between the individual and the organization, or for the implementation of pre-contractual measures taken in response to the data subject's request; or
(d) The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the organization and a third party; or
(e) All of the following apply: the transfer is for the benefit of the individual; it is reasonably impracticable to obtain the consent of the data subject to that transfer; if it were reasonably practicable to obtain such consent, the individual would be likely to give it.

Conclusion:

Due to the borderless nature of the internet and the ability of computers to collect, distribute and store vast volumes of electronic data, it is desirable that the processing of personal information is regulated to protect both, data collectors and data subjects. Data protection laws are particularly important to help protect privacy rights of individuals.

South Africa has made progress over the last decade to catch up on international developments relating to data and privacy protection laws.

The Protection of Personal Information Bill is expected to come into force in the course of 2010 and should, in the writer's view, align South African laws with international standards and the EU Directive relating to the protection of personal information.

Author: Emmie de Kock
15 January 2010