

A Short Walk Through the Protection of Personal Information Bill

BG *Bowman Gilfillan*
Attorneys

Eva Mudely
7 March 2011

Why 'POPIA'?

- Common law and Constitutional right to privacy
 - Personality right
 - Protected on piecemeal basis through case law
- Legislation of major trading partners requires adequate protection of personal information
 - Ease cross-border transactions

What is “Personal Information”

- Information relating to an identifiable, living natural person
- Information relating to an identifiable existing juristic person as far as applicable
- Not whether the information is readily obtainable that is important – focus is on nature of information
- Thus “personal” not only “private” information that is protected

“Personal Information”

- information related to the person’s race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture and birth;
- information relating to the person’s education or medical, financial, criminal or employment history;
- any identifying number, symbol, e-mail address, physical address, telephone number or other particular assigned to the person;
- the blood type or any other biometric information of the person;
- the personal opinions, views or preferences of the person;
- the views or opinions of another individual about the person;
- correspondence sent by the person that is implicitly or explicitly of a private/confidential nature, or further correspondence that would reveal the contents of the original correspondence;
- the name of the person if it appears with other personal information relating to the person, or if the disclosure of the name itself would reveal information about the person.

What is “Processing”?

- Any activity concerning personal information, e.g.
 - the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
 - dissemination by means of transmission, distribution or making available in any other form;
 - merging, linking, blocking, degradation, erasure or destruction of information.

Are all processing activities covered

- No, only the processing of personal information:
 - that is entered into a “record”;
 - by or on behalf of a responsible party that is:
 - Domiciled in South Africa
 - If not domiciled in South Africa, using automated or non-automated means situated in South Africa.

What is a “record”?

- Any recorded information in possession or control of responsible party, regardless of the medium and regardless of when it came into existence, i.e.:
 - In writing on any material
 - Information produced, recorded or stored by means of a tape-recorded, computer equipment
 - A label, marking or other writing that identifies or describes any thing of which it forms part
 - Books, maps, plans, graphs or drawings

Who are the role players?

- **Data Subject:** the person to whom the information relates
- **Responsible Party:** a private or public body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;
- **Operator:** a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of the responsible party
- **Regulator:** The Information Protection Regulator established by POPIA

Further restrictions on application

- **Not covered:**
 - Purely household activity
 - Information that has been de-identified, meaning that any information that identifies a particular person has been deleted (or that other information that may be used or manipulated to identify the person has been deleted)
 - Information by or on behalf of the State which involves national security, defence or public safety, or the purpose of which is the prevention, investigation or proof of offences, the prosecution of offenders or the execution of sentences
 - Processing for purely journalistic purposes by responsible parties who are subject, by virtue of office, employment or profession, to a code of ethics that provide adequate safeguards for the protection of personal information

The 8 Protection Principles

- Accountability
- Purpose specification
- Processing limitation
- Further processing limitation
- Information quality
- Openness
- Security safeguards
- Data subject participation

The 8 Protection Principles (cont)

- **Accountability**
 - The responsible party must ensure compliance
- **Purpose specification**
 - Must be collected for specific, explicitly defined and lawful purpose related to function/activity of responsible party
 - Data subject aware
 - Subject to certain exceptions, retain only for as long as is necessary for achieving the purpose

The 8 Protection Principles (cont)

- Processing limitation
 - Must be lawful
 - Must be done in reasonable manner that does not infringe the privacy of the data subject
 - Must be adequate, relevant and not excessive given the purpose
 - Consent or necessity
 - If consent: voluntary, specific, informed
 - Collection directly from data subject ... BUT NOT if
 - Would prejudice lawful purpose
 - Information contained in public record, etc

The 8 Protection Principles (cont)

- Further processing limitation
 - Further processing must be compatible with the purpose for which it was collected
 - How assessed?
 - Relationship between the purposes
 - Nature of information
 - Consequences for data subject
 - Manner in which information was collected
 - Any contractual rights between the parties

The 8 Protection Principles (cont)

- Further processing limitation (cont)
 - IS compatible if:
 - Data subject consented
 - Info available in public record or deliberately made public by data subject
 - Necessary in sphere of state security and punishment of offences, etc
 - Necessary to prevent threat to public health or life or health of data subject
 - Info used for historical, statistical or research purposes

The 8 Protection Principles (cont)

- Information quality

The responsible party must take reasonably practicable steps to ensure that the information is:

- Complete;
- Accurate;
- Not misleading; and
- Updated where necessary

The 8 Protection Principles (cont)

- Openness
 - Must notify the Regulator
 - Only needs to notify once, not each instance of processing, but if processing is different than initially notified, must notify within 1 year
 - Must notify Regulator re:
 - Processing for purposes of credit reporting, criminal behaviour
 - Transferring special personal info to countries without adequate protection laws
 - Regulator will then conduct a prior investigation

The 8 Protection Principles (cont)

- Openness (cont)
 - Must take reasonable steps to notify the data subject of:
 - Information being collected
 - Purpose for which information is collected
 - Whether supply of information is voluntary or mandatory
 - Consequences of failure to provide information
 - Any particular law that applies

The 8 Protection Principles (cont)

- Openness (cont)
 - Steps to inform the data subject must be taken:
 - Before collection if info is collected from data subject;
 - In other cases, before collection or as soon as reasonably practicable
 - Non-compliance is permitted inter alia if:
 - Data subject has consented
 - Non-compliance will not prejudice the legitimate interests of the data subject;
 - Compliance would prejudice a lawful purpose.

The 8 Protection Principles (cont)

- Security safeguards
 - Responsible party must secure the integrity of personal information by taking appropriate, reasonable technical and organisational measures to prevent
 - Loss, damage or unauthorised access
 - Unlawful access to or processing of personal information
 - The responsible party must take all reasonable measures to:
 - identify all reasonably foreseeable internal and external risks;
 - establish and maintain appropriate safeguards against the risks;
 - regularly verify that the safeguards are adequately implemented;
 - ensure the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards

The 8 Protection Principles (cont)

- Security safeguards (cont)
 - Information processed by an operator:
 - Responsible party must be aware;
 - Operator must treat information confidentially
 - Responsible party must ensure that the operator establishes and maintains appropriate security safeguards.
 - Processing by an operator must be governed by a written contract
 - In the event of security breaches, the responsible party must notify the Regulator and the data subject

The 8 Protection Principles (cont)

- Data subject participation
 - Data subjects' rights:
 - Request confirmation whether information is held;
 - Request description of information held;
 - Request confirmation of recipients
 - Responsible party may refuse on basis of grounds in PAIA
 - Data subject may request a responsible party to:
 - correct or delete personal information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully;
 - destroy or delete a record that the responsible party is no longer entitled to retain.
 - The responsible party must comply with the request, or attach the request to the information not amended as requested.

Special Personal Information

- What is “special personal information”?
 - religious or political beliefs;
 - race or ethnic origin;
 - trade union membership;
 - political opinions;
 - **health, sexual life;**
 - criminal behaviour.

Special Personal Information (cont.)

- Religious or philosophical beliefs
 - Processing may take place by:
 - spiritual or religious organisations, provided that the information concerns data subjects belonging to such organisations;
 - institutions founded on religious or philosophical principles with respect to their members or other members belonging to such institution, if it is necessary to achieve their aims and principles; or
 - other institutions, provided that it is necessary to protect the spiritual welfare of the data subjects, unless they have objected to the processing.
 - The information may not be supplied to 3rd parties without the data subject's consent.

Special Personal Information (cont.)

- **Race**
 - Processing may be carried out to:
 - Identify data subjects when this is essential;
 - Comply with laws or measures designed to protect or advance persons disadvantaged by unfair discrimination
- **Trade union membership**
 - Processing may take place by a trade union to which the data subject belongs, or the trade union federation to which the trade union belongs, if the processing is necessary to achieve the aims of the trade union/trade union federation.
 - The information may not be supplied to third parties without the consent of the data subject

Special Personal Information (cont)

- Political persuasion
 - Processing may take place by an institution founded on political principles if such processing is necessary to achieve the aims or principles of the institution.
 - The information may not be supplied to third parties without the consent of the data subject.

Special Personal Information (cont)

- Health or sexual life
 - Processing may take place by:
 - Medical practitioners, healthcare institutions
 - Insurance companies, medical aid scheme providers
 - Schools
 - Institutions of probation, child protection or guardianship
 - Minister of Justice and Minister of Correctional Services
 - Pension funds and employers if processing is necessary for:
 - Implementation of laws/pension regulations
 - Reintegration/support for workers or persons entitled to benefit in connection with sickness/work incapacity
 - Processing must be confidential

Special Personal Information (cont)

- Criminal behaviour
 - Processing may take place by:
 - bodies charged by law with applying criminal law;
 - responsible parties who have obtained the information in accordance with the law;
 - responsible parties who process the information for their own lawful purposes to:
 - assess an application by a data subject in order to take a decision about or provide a service to that data subject;
 - protect their legitimate interests in relation to criminal offences.

General Exemption

- Regulator
 - The Regulator may authorise processing and such processing will not be in breach of POPIA
 - The public interest include:
 - the legitimate interests of State security;
 - the prevention, detection and prosecution of offences;
 - important economic and financial interests of the State or a public body;
 - historical, statistical or research activity.

Cross Board Transfers

Cross border transfers of personal information may only take place: if

- the recipient is subject to a law, binding code of conduct or contract which:
 - effectively upholds the principles for reasonable processing that are substantially similar to the information protection principles; and
 - includes provisions relating to the further transfer of personal information that are substantially similar to what is contained in POPIA;
- the data subject consents;
- the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data-subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject; or
- the transfer is for the benefit of the data subject and:
 - it is not reasonably practicable to obtain the data subject's consent; and
 - if it were reasonably practicable, the data subject would be likely to give it.

Consequences of Non-Compliance

- The data subject may lodge a complaint with Regulator
- The Regulator may try and secure settlement
- If no settlement possible, the Regulator may initiate investigation
- If breach, the Regulator may issue enforcement notice
- Data subject / Regulator may sue responsible party for damages
- Uncertain what amounts would be awarded, but court would be entitled to award:
 - Damages for patrimonial and non-patrimonial loss
 - Aggravated damages
 - Interest
 - Legal fees

Offences & Penalties

- **Offences:**
 - obstructing or unlawfully influencing the Regulator;
 - Breach by persons acting for Regulator of duty of confidentiality;
 - Failure to comply with enforcement notice
 - Making false statements
- **Penalties**
 - 10 years/fine or both
 - 12 months/fine or both

When do we need to be compliant?

- Not certain when POPIA will become law, but anticipated to be in 2011
- Transitional period of at least 1 year envisaged.

Focus on POPIA Security Safeguards

- Enforcement Powers – The European Union
- Enforcement Powers – The United Kingdom
 - UK Law
 - Recent Information Commission investigations
 - Criminal Case Law
 - Launching criminal proceedings is used by the Commission as a last resort

- Security safeguards
 - Responsible party must secure the integrity of personal information by taking appropriate, reasonable technical and organisational measures to prevent
 - Loss, damage or unauthorised access
 - Unlawful access to or processing of personal information

- The responsible party must take all reasonable measures to:
 - identify all reasonably foreseeable internal and external risks;
 - establish and maintain appropriate safeguards against the risks;
 - regularly verify that the safeguards are adequately implemented;
 - ensure the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards
- Information processed by an operator:
 - Responsible party must be aware;
 - Operator must treat information confidentially
- Responsible party must ensure that the operator establishes and maintains appropriate security safeguards.
- Processing by an operator must be governed by a written contract
- In the event of security breaches, the responsible party must notify the Regulator and the data subject

Enforcement Powers – The United Kingdom

- Highlights of Data Protection and Privacy Enforcement In 2009 and 2010
- The Association of Teachers and Lecturers
 - This matter concerns a laptop computer and a memory stick which were lost or stolen from the roadside as an ATL staff member was packing his car
 - The laptop, which was not encrypted but was password protected, was the property of ATL and contained sensitive personal data relating to some 6,282 union members
 - The memory stick in question was personally owned by the ATL member of staff, and contained 3,366 of the laptop records. The memory stick was not password protected or encrypted

- The Information Commissioner ruled that:
 - Portable and mobile devices including laptops and other portable media used to store and transmit personal data, the loss of which could cause damage or distress to individuals, are encrypted
 - The policy covering the transfer, storage and use of personal data is reviewed to ensure compliance with the Act, particularly in respect of the security of the means of transfer and relevance of the data transferred
 - Staff must be made aware of the data controller's policy for the storage, use and transfer of personal data and are appropriately trained how to follow that policy
 - Staff will be prohibited from storing data on personal memory sticks

- **Mr Ian Kerr trading as The Consulting Association**
 - The Commissioner was informed that a list was operating within the construction industry. It was alleged that contractors in the construction industry would send a list of the names of potential staff to the data controller who would then check the names against a list and then advise the contractors of intelligence information which the data controller held in relation to those named on that list. The contractor would then make a decision whether or not to employ an individual on the basis of that information
 - A search of the premises by the Commissioner revealed a ring binder containing 3,213 entries in relation to individuals. The entries contained information such as names, dates of birth, national insurance numbers, locations and trades alphabetically, as well as union activity listed on pages which had been processed on electronic media

- **The Information Commissioner ruled that:**
 - Mr. Kerr processed personal data unfairly by failing to notify the individuals whose names are on the list that he had information about them
 - Damage or distress to the individuals named on the list is likely as a result of them not being aware of the existence of the list and being denied the opportunity of explaining or correcting what may be inaccurate personal data about them
 - Mr. Kerr was to refrain from obtaining, using or disclosing any personal data unless the disclosure is necessary for the purpose of complying with any obligation under the Act
 - Mr. Kerr was to refrain from altering, erasing or destroying any personal data

- Secretary of State for the Home Department
 - The Commissioner was informed of the loss of an unencrypted memory stick holding, in all likelihood, the sensitive personal data of prisoners and offenders
 - The memory stick went missing whilst under the control of PA Consulting Group who was working under contract to the Home Office and processing the data on its behalf

- The Information Commissioner ruled that:
 - Where processing of personal data is carried out by a data processor on behalf of the data controller, the data controller shall take reasonable steps to ensure compliance with the guarantees made by the data processor in respect of the technical and organisational security measures governing the processing to be carried out
 - In taking reasonable steps the data controller shall carry out and document regular inspections of the security of the data processor's facilities for the processing of personal data and carry out regular audits of the data processor's processing activities to ensure compliance

- Camden Primary Care Trust
 - The Commissioner was informed of an incident involving the loss of redundant personal computers holding the sensitive personal data (including names, addresses and medical diagnoses) of over 2,500 individuals
 - The personal computers had been left by a skip inside the grounds of St. Pancras Hospital for a period of 13 days before the data controller discovered that they had been removed without its authority

- The Information Commissioner ruled that:
 - The Trust ensure that any personal data is expunged from computer equipment as soon as it has been decommissioned, for example, by removal and destruction of the hard drives

- The University of Manchester

- The Information Commissioner was provided with a report regarding the accidental publication of a spreadsheet which contained the personal data of some 1,755 students. This data included information relating to certain students ‘disabilities’
- The information was published when a member of the University staff accidentally sent it as an attachment to an email, forwarded to some 469 students
- The information accidentally published was forwarded to the staff member by a colleague, when they had requested a list of the email addresses of certain students. An extract of the full student record was provided, despite the fact that the staff member had no business need to acquire the full information

- The Information Commissioner ruled that:
 - The University shall take all reasonable measures to ensure the physical security of personal data being processed in furtherance of the duties of the University of Manchester
 - The University shall ensure that its policies on the transfer, sharing and publication of personal data are clear and that staff are adequately trained on how to fulfill their obligations under such policies
 - The University shall implement such other security measures it deems appropriate to ensure that personal data is protected against unauthorised and unlawful process, accidental loss, destruction, and/or damage

- Imperial College Healthcare NHS Trust
 - The Information Commissioner was provided with a report from the Trust regarding the theft of 6 laptop computers (in two separate incidents of theft) and the loss of a small number of paper records which contained, in total, personal data relating to some 6,000 of the Trust's patients
 - One laptop computer, which was not Trust owned, was password protected but was unencrypted. It contained data relating to medical treatment
 - The laptop computers were stolen by means of burglary from a secure area within the hospital. The paper records were contained within a cycle pannier which was lost in transit

- The Information Commissioner ruled that:
 - Portable and mobile devices including laptops and other portable media used to store and transmit personal' data, the loss of which could cause damage or distress to individuals, are encrypted using encryption software

- East Cheshire NHS Trust

- The Commissioner received a report that pages from an A&E register, containing personal data relating to over 60 patients, was found in a garden in Newcastle-under-Lyme
- This followed an office move involving various departments of the Trust, including A&E, during which an external company was retained to clear out scrap and rubbish from vacated premises
- The data controller did not enter into any written contract with the external company, nor were its actions appropriately supervised. It was noted during the clearance operations that boxes of documents were being disposed of in open skips, but the data controller failed to react to this in time to prevent loss of some records

- The Information Commissioner ruled that:
 - In all cases where third party suppliers of goods or services will have access to personal data, a written contract is entered into prior to work commencing, which covers the requirements of the Act
 - All staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained how to follow that policy

Security Implementation Checklist

- Security implementation checklist:
 - Establish a documented and auditable routine to:
 - Identify all reasonably foreseeable internal and external risks;
 - Establish and maintain appropriate safeguards against the risks;
 - Encryption (make sure that your solution is ECT Act compliant)
 - Password protection
 - Physical destruction
 - Regularly verify that the safeguards are adequately implemented;

- Ensure the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards
 - In the event of security breaches, the responsible party must notify the Regulator and the data subject
- Where information is processed by a third party:
- The data controller must be aware
 - Third party must treat information confidentially

- The data controller must ensure that the operator establishes and maintains appropriate security safeguards
 - Password protection
 - Encryption (make sure that your solution is ECT Act compliant)
 - Physical destruction
 - Inspection of the third party's premises, systems and compliance
- Processing by an operator must be governed by a written contract
- In the event of security breaches, the responsible party must notify the Regulator and the data subject