The management of personal data in the workplace is soon to be regulated by the provisions of a *Protection of Personal Information Act*. A draft bill was published for comment in 2005. Following public comment, the bill was refined by the South African Law Reform Commission and has been submitted to the Department of Justice for its consideration and further reflection, prior to its introduction into Parliament and enactment into law, anticipated sometime in 2009.

**WHAT IS PERSONAL INFORMATION?**

Before reflecting on why it is important to protect personal information and how this is to be achieved, it is useful to understand what ‘personal information’ is. Personal information, or personal data, as it is sometimes called, is defined in the *Protection of Access to Information Act* 2 of 2000 (PAIA), which definition is mirrored in the *Protection of Personal Information Bill* (Bill).

‘Personal information' is defined as ‘information about an identifiable, natural person, and in so far as it is applicable, an identifiable, juristic person, including, but not limited to:

a) information relating to the 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, language and birth of the person;

b) information relating to the education or the medical, criminal or employment history of the person or information relating to financial transactions in which the person has been involved;

c) any identifying number, symbol or other particular assigned to the person;

d) the address, fingerprints or blood type of the person;

e) the personal opinions, views or preferences of the person, except where they are about another individual or about a proposal for a grant, an award of a prize to be made to another individual;

f) correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

---

*Paper prepared by: Debbie Collier and Rufaro Gweshe, Institute of Development and Labour Law, Faculty of Law, University of Cape Town.*

*The draft Protection of Personal Information Bill has been published on the conference CD.*

*The same definition is contained in s 1 of the Electronic Communications and Transactions Act 25 of 2002.*
g) the views or opinions of another individual about the person;

h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the person, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

i) the name of the person where it appears with other personal information relating to the person or where the disclosure of the name itself would reveal information about the person;

j) but excludes information about a natural person who has been dead, or a juristic person that has ceased to exist, for more than 20 years...’

WHY SHOULD WE CONCERN OURSELVES WITH PERSONAL INFORMATION?

Personal information is protected through the right to privacy. There’s nothing new about the right to privacy: it is enshrined in the Constitution and in the common law. Section 14 of the Constitution states that ‘everyone has the right to privacy, which shall include the right not to have their person or home searched; their property searched; their possessions seized; or the privacy of their communications infringed’. It has been held by the courts that it is section 14(d) in particular which ‘protects information to the extent that it limits the ability to gain, publish, disclose or use information about others’.3

Data protection is a matter of international concern and is the subject of much international and foreign law regulation which in turn requires South Africa to do the same4 before allowing personal data to flow other our borders. For example, the European Council’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; the Organisation for Economic Co-operation and Development’s Guidelines Governing the Protection of Privacy and the Transborder Flows of Personal Data; and the European Union’s Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, all set the standard for data protection. Once the Protection of Personal Information Bill (Bill) is enacted, South Africa law should meet the standards set in these international instruments.

The South African Law Reform Commission (SALRC) drafted the Bill to establish the mechanisms and procedures that will bring South Africa in line with international conventions, in a manner that complies with the right to privacy in section 14(d) of the Constitution.5 The Bill is due to come before Parliament sometime in 2009. The proposed legislation will apply to anybody who processes6 personal information within

---


4 The data protection principles are incorporated into South Africa’s Electronic Communications and Transactions Act 25 of 2002. In this context, they may be voluntarily subscribed to which regard to personal data collected via electronic transactions.

5 Clause 1 Protection of Personal Information Bill.

6 Processing is defined in the Bill as the ‘collection, recording, organisation, storage, updating or modification, retrieval, consultation, use, dissemination by means of transmission, distribution or
South Africa, as well as anybody who processes information within South Africa on behalf of bodies outside of South Africa. The Bill also binds the State. The 'international prescripts' which the Bill seeks to be in harmony with are the universally recognised information protection principles.

THE INFORMATION PROTECTION PRINCIPLES

These intertwined principles appear in a number of configurations that embrace the same ideas about data privacy and generally form the basis of almost every data protection law, be it domestic or international. The Protection of Personal Information Bill is no exception, and includes these principles in Chapter 3. This section will discuss the content of each principle whilst providing examples of how these principles can be successfully implemented in the workplace. The examples are based on the UK's Employment Practice Code which implements the information protection principles in the UK. These principles should inform the manner in which all employee information is processed in the workplace, including information relating to:

- Recruitment and selection – job applications and pre-employment processes
- Employment records – the collection, storage, disclosure and deleting of records
- Workplace monitoring – monitoring use of telephones, internet, e-mail systems, motor vehicles etc
- Health – occupational health, medical testing, drug and genetic screening.

The processing of such information should take place in accordance with the information protection principles, which, in the South African context, are encapsulated in Chapter 3 in the following format:

- Principle 1 Processing limitation
- Principle 2 Purpose specification
- Principle 3 Further processing limitation
- Principle 4 Information quality
- Principle 5 Openness
- Principle 6 Security safeguards
- Principle 7 Individual participation
- Principle 8 Accountability

These principles are discussed more broadly below, in the context of the principles as universal principles, together with examples of their implementation in the workplace, which examples are drawn from the UK approach.

1) Processing limitation
The first principle indicates that processing must be lawful and not excessive (the principle of minimality). Data processing will only occur lawfully if the conditions that making available in any other form, merging, linking, as well as blocking, erasure or destruction of information'.

7 These examples are simply illustrative and not exhaustive. It is likely that South Africa will in due course have its own codes of practice. Until such time, the UK code may be used to establish good practice.
justify the processing are satisfied. The unauthorised processing of data is wrongful. In South Africa some of the traditional grounds of justification which are appropriate in the context of fair and lawful processing are consent, private defence, necessity and statutory or official capacity. The maintenance and furtherance of a legitimate private interest or of the public interest has been considered as another ground.

The UK Data Protection Act provides the following as lawful ways of processing information:

i. Data subject has provided consent (this can be express or implied, for example if you do not tick an ‘opt out’ box at the bottom of a web page).

ii. Where the processing is necessary for the performance of a contract.

iii. Where the processing is necessary to protect your vital interests. The Information Commissioner’s Office in the United Kingdom states, in its Code of Good Practice, that this condition may only be claimed "where the processing is necessary for matters of life and death, for example, the disclosure of a data subject’s medical history to a hospital casualty department treating the data subject after a serious road accident".

iv. Where the processing is necessary for the completion of public functions including the administration of justice and the exercise of any functions of a government department.

---

Example 1: Providing References

The UK Information Commissioner’s Office suggests that employers comply with the procedures outlined below in order to process information lawfully and fairly. When an employer is asked to provide a reference for an employee:

- Do not provide confidential references about a worker unless you are sure that this is the worker’s wish.
- Set out a clear company policy stating who can give corporate references, in what circumstances, and the policy that applies to the granting of access to them.
- Make anyone who is likely to become a referee aware of this policy.
- As part of the policy, include a requirement that all those giving corporate references must be satisfied that the worker wishes the reference to be provided.
- As part of an Exit Policy, include on file a record of whether the worker wishes references to be provided after he/she has left.


---

9 Supra.
10 Roos (note 4) at 109.
11 Roos (note 4) at 110.
In addition, only personal data that is really necessary for the purpose stated should be collected. It is also generally not acceptable for employers to hold information on the basis that it might possibly be useful in the future.

**Example 2: Recruitment Records**

- When advertising for a vacancy, only seek personal information that is relevant to the recruitment decision to be made.
- Determine whether all questions are relevant for all applicants.
- Consider customising application forms where posts justify the collection of more intrusive personal information.
- Remove or amend any questions which require the applicant to provide information extraneous to the recruitment decision.
- Remove questions that are only relevant to people your organisation goes on to employ (e.g. banking details) but are not relevant to unsuccessful applicants.
- Assess who in your organisation retains recruitment records (e.g. are they held centrally, at departmental level or in the line).
- Ensure that no recruitment record is held beyond the statutory period in which a claim arising from the recruitment process may be brought unless there is a clear business reason for exceeding this period.
- Consider anonymising any recruitment information that is to be held longer than the period necessary for responding to claims.
- Check who in your organisation retains information from vetting. Ensure that vetting records are destroyed after 6 months. Manual records should be shredded and electronic files permanently deleted from the system.
- Inform those responsible for the destruction of this information that they may keep a record that vetting was carried out, the result and the recruitment decision taken.
- Ensure that application forms or surrounding documentation tell applicants that, should they be unsuccessful, their details will be kept on file unless they specifically request that this should not be the case.


2) Purpose specification

Data may only be processed for specified and lawful purposes and may not be subsequently processed in ways that are inconsistent with these purposes. It is necessary to define/specify the purposes for which the data is collected; and these purposes must be lawful/legitimate. Data must also not be retained for longer than is necessary to achieve the stated purpose; unless there are lawful reasons for doing so.

---

13 Roos (note 4) at 111. In South Africa, the later is encapsulated in the ‘further processing limitation’ principle.
15 Supra.
Therefore in practice, the employer must have a valid reason to collect your personal data and (s)he must inform the employee/job applicant what that reason is. In addition to this, employees cannot collect personal information for one reason, and then use that information for another unrelated purpose.\footnote{The Liberty Guide to Human Rights ‘Overview of data protection principles’. Available at http://www.yourrights.org.uk/yourrights/privacy/data-protection/overview-of-data-protection-principles.shtml. [Accessed 22/07/2009].}

### Example 3: Discipline and Dismissals

The Protection of Personal Information Bill applies to the collection of personal information in any context, including disciplinary and dismissal proceedings. The following guidelines are provided by the Information Commissioner’s Office in the United Kingdom and are a useful example of how to conduct disciplinary and dismissal proceedings in accordance with the purpose specification principle and the proposed legislation:

- First, employers need to assess the company's disciplinary procedures and grievance procedures and decide whether the existing procedures comply with the Bill.

- Employers need to ensure that whoever (whether this be another employee of the company or an outsourced company) is responsible for collecting information to be used in these types of proceedings is aware that the proposed legislation grants employees the right to access any personal information and that when they gather the information they have a duty to disclose the purpose for which they are gathering the information.

- Employers must note that they should not use or access information collected for the purposes of disciplinary or dismissal proceedings if such access or use would be incompatible with the purpose(s) that the information was obtained for.

The Information Commissioner’s Office ‘Employment Practice Code’. Available at www.ico.gov.uk. [Accessed 22/07/09]

### Case Study 1

Following the suggestion by Professor Rycroft in Moonsamy v The Mailhouse would also ensure that employers comply with the Protection of Personal Information Bill when collecting information for a disciplinary hearing or a dismissal. In this case the employer intercepted the telephone conversations of his employee by using a listening and recording device (a 'tap' or 'bug') that was connected to the employee’s telephone in his office at the premises of the employer. The conversations collected from the wire tap were subsequently led as evidence at the employee's disciplinary hearing. The chairperson at the hearing relied on the evidence from the wire tap as well as other evidence when they decided that the dismissal of the employee was the appropriate sanction. The employee approached the CCMA for relief, and it was held that the employer could have achieved his goal by using less restrictive means. The Commissioner arbitrating the matter suggested that the employer could have obtained the consent of an employee (at the inception of the employment agreement, or through a consensual amendment to an existing employment agreement), allowing the employer to monitor any conversation on the employer's telephones. The consent obtained, which would in most cases form an express or implied term and condition of employment, would have to be such that the employee has a full appreciation of the nature and extent of the act to which he or she is voluntarily consenting.

From Moonsamy v The Mailhouse (1999) 20 ILJ 464 (CCMA)
3) **Further processing limitation**
The further processing limitation principle prohibits the processing of data in a manner incompatible with the purpose for which it was collected. This will include a limitation on the onward transmission of the data to a third party. The bill provides a number of circumstances in which the processing of data would not be incompatible with the purpose for which it was collected, for example for the enforcement of law and in the conduct of court proceedings.

4) **Information quality**
The data should be valid regarding what it is intended to describe, thus it must be relevant, accurate and up to date with respect to the purposes for which it will be processed. Employers must therefore ensure that obsolete and erroneous information is removed or updated.

---

### Example 4: Keeping General Records

The guidelines below are recommendations made by the Information Commission’s Office in the United Kingdom.

- Provide each worker with a copy of information that may be subject to change, e.g. personal details such as home address, annually or allow workers to view this on-line.
- Ask workers to check their records for accuracy and ensure any necessary amendments are made to bring records up-to-date.
- Decide whether data that change could easily be viewed electronically and make any changes to systems necessary to enable this.
- Ensure that the system restricts access to individuals’ records so that each worker can only get access to his or her own record.
- Make provision to amend any details that are incorrect on individual workers’ files.
- Incorporate accuracy, consistency and validity checks into systems.
- Remember that legal responsibility for data protection compliance rests with users rather than suppliers of systems.

---

5) **Openness / Transparency**
This principle ensures that employees or job applicants, whatever the case may be, are notified when their data is being processed, are informed about the purpose for which it is processed, know the identity of the recipients of their personal data as well as the identity and regular address of the employer. The bill requires the appointment of a responsible party and the notification of the collection of data to the Commission.

---

17 Roos (note 4) at 114.
19 Roos (note 4) at 116.
**Example 5: Applications**

The following is provided by the UK’s Information Commissioner’s as an example of how to ensure job applications comply with this data protection principle.

- Inform job applicants of the name of the organisation to which they will be providing their information and how it will be used unless this is self-evident.
- Ensure that the name of the organisation appears in all recruitment advertisements.
- Ensure that the organisation is named on the answer phone message which invites potential applicants to leave details.
- Ensure that the organisation is named on the website before personal information is collected on an online application form.
- To the extent that it is not self evident describe in the advertisement the purposes for which the organisation may use personal information, for example, to market the organisation’s products and service.
- Recruitment agencies, used on behalf of an employer, should identify themselves and explain how personal information they receive will be used and disclosed unless this is self-evident.
- If you use a recruitment agency check that it identifies itself in any advertisement, and that it informs applicants if the information requested is to be used for any purpose of which the applicant is unlikely to be aware.
- On receiving identifiable particulars of applicants from an agency ensure, as soon as you can, that the applicants are aware of the name of the organisation holding their information.
- Inform the applicant as soon as you can of the employer’s identity and of any uses that the employer might make of the information received that are not self-evident.
- OR
- If the employer does not wish to be identified at an early stage in the recruitment process, ensure the agency only sends anonymised information about applicants. Ensure the employer is identified to individuals whose applications are to be pursued further.


6) **Security safeguards**

In order to comply with this, principle employers must ensure that personal data is protected by reasonable security safeguards against risks such as the loss or unauthorised access, destruction, use, modification or disclosure of data.\(^{20}\)

**Example 6:**

The Information Commissioner’s Office in the United Kingdom advises employers to ensure that they take the steps below in order to ensure their systems meet the necessary security levels.

- Ensure that security standards take account of the risks of unauthorised access to,
The accidental loss of, destruction of, or damage to employment records.

- Institute a system of secure cabinets, access controls and passwords to ensure that staff can only gain access to employment records where they have a legitimate business need to do so.

- Check whether computerised systems that retain personal information currently have audit trail capabilities. If they do, check that the audit trail is enabled.

- If they do not, see if it would be possible to create audit trails of who accesses and amends personal information.

- If you have a system with audit trails, ensure that regular checks occur to detect unauthorised or suspicious use. Set up a procedure to investigate patterns of unusual or unauthorised access of personal information.

- Take steps to ensure the reliability of staff that have access to workers’ records.

- Ensure that if employment records are taken off-site, e.g. on laptop computers, this is controlled. Make sure only the necessary information is taken and there are security rules for staff to follow.

- Take account of the risks of transmitting confidential worker information by fax or e-mail. Only transmit information between locations if a secure network or comparable arrangements are in place.


---

7) **Individual (data subject) participation**

Employees and job applicants should be allowed to participate in and have a measure of influence over the processing of their personal data.21

---

### Example 7: Employee’s Access to Information

These are the guidelines set out for employers by the UK Information Commissioner’s Office.

- Establish a system that enables the organisation to recognise an employee’s access request and to locate all the information about a worker in order to be able to respond promptly and in any case within 40 calendar days of receiving a request.

- Check the identity of anyone making a subject access request to ensure information is only given to the person entitled to it.

- Provide the worker with a hard copy of the information kept, making clear any codes used and the sources of the information.

- Ensure that the information supplied is intelligible, that it includes sources and that if at all possible it is in hard copy form.

- Make a judgement as to what information it is reasonable to withhold concerning the identities of third parties.

- Inform managers and other relevant people in the organisation of the nature of information that will be released to individuals who make subject access requests.

---

21 Roos (note 4) at 119.
Ensure that on request, promptly and in any event within 40 calendar days, workers are provided with a statement of how any automated decision-making process, to which they are subject, is used, and how it works.

When purchasing a computerised system ensure that the system enables you to retrieve all the information relating to an individual worker without difficulty.

The Information Commissioner’s Office ‘Employment Practice Code’. Available at www.ico.gov.uk. [Accessed 22/07/09]

8) Accountability (and sensitivity)
In the Bill, the accountability principle requires the responsible person to ensure compliance with the principles. In addition, the accountability principle recognizes that the processing of certain types of information, regarded as especially sensitive, is subjected to more stringent controls. The principle ensures that the final responsibility for compliance rests with the employer, even in instances where the employer has entrusted the data collection process to an employee or to a third party.

Dealing with Sensitive (‘Special’) Information
The Bill places limitations on the collection of the following types of personal information, regarded as ‘special information’:

- religion or philosophy of life,
- race,
- political persuasion,
- health
- sexual life,
- personal information concerning trade union membership,
- criminal behaviour and,
- unlawful or objectionable conduct connected with a ban imposed with regard to such conduct.

The ‘special information’ may only be processed under certain conditions. These conditions are found in clauses 25 – 31 of the Bill. They provide exemptions to the prohibition. The exemptions are listed as follows:

Religion or philosophy of life – the exemption in clause 25 allows religious, philosophical and spiritual institutions to process personal information regarding a person’s religious and philosophy of life.

Race – clause 26 allows the employer to process information concerning a person’s race if it is essential to identify a person’s race and for EE or AA purposes.

Political persuasion – according to clause 27 only political institutions are allowed to access information concerning a person’s political persuasion.

Personal information concerning trade union membership - in terms of clause 28 only trade unions and trade union federations can access information concerning a person’s trade union membership.

Health – clause 29 permits amongst others, employers or institutions working for them to access personal information concerning a person’s health and sexual life under specific conditions.

---

22 Roos (note 4) at 121.
23 Supra.
Criminal behaviour – it is only those bodies, charged by law with applying criminal law and by responsible parties who have obtained personal information in accordance with the law who can access personal information concerning a person’s criminal behaviour. Clause 30 also allows other bodies to access the information if it is in line with the subsections 2 – 5.

Clause 31 – lists the general exemptions applicable to the processing of special personal information. In terms of this clause processing ‘special information’ is permitted where:

(a) it is carried out with the express consent of the data subject;
(b) the information has manifestly been made public by the data subject;
(c) it is necessary for the establishment, exercise or defence of a right in law;
(d) it is necessary to comply with an obligation of international public law, or
(e) it is necessary with a view to an important public interest, where appropriate guarantees have been put in place to protect individual privacy and this is provided for by law or else the Commission has granted an exemption.

REGULATORY ASPECTS

The following regulator aspects of the Bill are worth noting:

1) The creation of an Information Protection Commission

The Bill provides for the establishment of an Information Protection Commission. This Commission is to be made up of three individuals appointed by the State President, and it will be chaired by the Information Commissioner. The commission will be granted the following powers and duties:

- **Educational**
  To promote via education and publicity an understanding and acceptance of the information privacy principles and their objects.

- **Monitor**
  To monitor the compliance of public and private bodies of the provisions of this Act. To monitor and research developments in information processing and computer technology as a way of ensuring that any adverse effects of such developments on the protection of the personal information of persons are minimised.
  To monitor any proposed legislation (including subordinate legislation) or any proposed policy of the Government that may affect the protection of the personal information of individuals.
  To monitor the use of unique identifiers of data subjects, and to make recommendations to the Minister relating to the need of, or desirability of taking, legislative, administrative, or other action to give protection, or better protection, to the personal information of a person.

- **Reporting and Auditing**
  To report (with or without request) to the Minister from time to time on any matter affecting the protection of the personal information of a person, including the need for, or desirability of,
taking legislative, administrative, or other action to give protection or better protection to the personal information of a person.

To conduct an audit of personal information maintained by that body for the purpose of ascertaining whether or not the information is maintained according to the information privacy Principles when requested to do so by a public or private body.

To report to the Minister from time to time on the desirability of the acceptance, by South Africa, of any international instrument relating to the protection of the personal information of a person.

To report to the Minister on any other matter relating to protection of information that, in the Commission's opinion, should be drawn to the Minister's attention.

- **Examine Legislation**
  To examine any proposed legislation that makes provision for the collection of personal information by any public or private body; or the disclosure of personal information by one public or private body to any other public or private body, or both.

- **Consultation**
  To receive and invite representations from members of the public on any matter affecting the personal information of a person.

  To consult and co-operate with other persons and bodies concerned with the protection of information privacy.

  To act as mediator between opposing parties on any matter that concerns the need for, or the desirability of, action by one person in the interests of the protection of the personal information of another person.

  To provide advice (with or without a request) to a Minister or a public or private body on their obligations under the provisions, and generally, on any matter relevant to the operation, of this Act.

- **Complaints**
  To receive and investigate complaints about alleged violations of the protection of personal information of persons and in respect thereof make reports to complainants.

  To gather such information as in the Commission's opinion will assist the Commission in discharging the duties and carrying out the Commission's functions under this Act.

  To attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation.

  To serve any notices in terms of this Act and further promote the resolution of disputes in accordance with the prescripts of this Act.

- **Codes of Conduct**
  To issue, from time to time, codes of conduct, amendment of codes and revocation of codes of conduct.

  To make guidelines to assist bodies to develop codes of conduct or to apply codes of conduct.

  To review an adjudicator's decision under approved codes of conduct.

- **General**
  To do anything incidental or conducive to the performance of any of the preceding functions.

  To exercise and perform such other functions, powers, and duties as are conferred or imposed on the Commission by or under this Act or any other enactment.
2) **The appointment of Information Protection Officers**\(^{26}\)

The proposed legislation places a duty on all employers to ensure that they appoint one or more **Information Protection Officers** within the organisation, tasked with the following statutory duties:

- Encouraging compliance with the information protection principles;
- Dealing with requests made to the organisation in terms of the Bill;
- Working with the Commission in relation to investigations conducted in terms of the Bill and in relation to the organisation;
- Ensuring general compliance by the organisation with the provisions of the Bill.

The **Promotion of Access to Information Act 2 of 2000** regulates the appointment of Information Protection Officers in the public service. PAIA defines Information Protection Officers as Director-Generals, heads, executive directors or equivalent officers, can be appointed as Information Protection Officers. This suggests that only those who occupy managerial positions within an organisation can be appointed as Information Protection Officers.

3) **Penalties and offences**\(^{27}\)

The Bill envisages the following offences and penalties:

<table>
<thead>
<tr>
<th>Offences</th>
<th>Penalties</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is an offence to hinder, obstruct or unduly influence the Commission or any person acting on behalf or under the direction of the Commission in the performance of the Commission’s duties and functions under this Act. (Clause 88)</td>
<td>Contravention of clause 88 can lead to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and imprisonment. (Clause 91)</td>
</tr>
<tr>
<td>It is an offence to intentionally obstruct a person executing a warrant issued in terms of the Act. It is also an offence to fail to assist the person executing the warrant, without a reasonable excuse. (Clause 89)</td>
<td>Contravention of this clause can result in a fine or imprisonment for a period not exceeding 12 months, or both a fine and imprisonment. (Clause 91)</td>
</tr>
<tr>
<td>Failure to comply with an enforcement notice served on a responsible party, such as an employer, suspected of interfering with the protection of the personal information of a person is an offence. (Clause 90(1))</td>
<td>Contravention of this clause can result in a fine or imprisonment for a period not exceeding 12 months, or both a fine and imprisonment. (Clause 91)</td>
</tr>
<tr>
<td>If a responsible party is served with an information notice requesting the responsible party to furnish information on its personal information processes, knowingly or negligently makes a statement which is false in a material respect, they are guilty of an offence. (Clause 90(2))</td>
<td>Contravention of this clause can result in a fine or imprisonment for a period not exceeding 12 months, or both a fine and imprisonment. (Clause 91)</td>
</tr>
</tbody>
</table>

---

\(^{26}\) Clause 46(1) of the Protection of Personal Information Bill.

\(^{27}\) Chapter 9 of the Protection of Personal Information Bill.
The employers’ obligations arising out of the privacy attached to personal data are further regulated by the provisions of the Electronic Communications and Transactions Act 25 of 2002 (ECT Act) which, in s 86(1) makes it an offence to access or intercept data without authorisation, and the Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002 (the RIC Act), the relevant provisions of which are set out below.

### Monitoring employees: RIC Act limitations

The relevant provisions of the RIC Act provide as follows:

2. **Prohibition of interception of communication**
   … [interception must be authorised by a judge or the exceptions set out in this Act (see ss 5 & 6 below)], no person may intentionally intercept or attempt to intercept, or authorise or procure any other person to intercept or attempt to intercept … any communication in the course of its occurrence or transmission.

5. **Interception of communication with consent of party to communication**
   (1) Any person … may intercept any communication if one of the parties to the communication has given prior consent in writing …

('Intercept' means the … acquisition of the contents of any communication … and includes the –

a) monitoring … by means of a monitoring device;

b) viewing, examination or inspection of the contents of any indirect communication;

c) diversion … to another destination.)

6. **Interception of indirect “communication in connection with carrying on of business**
   (1) Any person may, in the course of carrying on of any business, intercept any indirect communication … *in the course of its transmission* over a telecommunication system.

(2) A person may only intercept an indirect communication in terms of (1) –

(a) if such interception is effected by, or with the … consent of the system controller;

(b) for the purposes of –

(i) monitoring or keeping a record of indirect communications –

(aa) in order to establish the existence of facts;

(bb) for purposes of investigating or detecting the unauthorised use of that telecommunication system; or

(cc) where that is undertaken in order to secure, or as an inherent part of, the effective operation of the system;

(ii) monitoring indirect communications made to a confidential voice-telephony counselling or support service which is free of charge, other than the cost, if any, of making a telephone call, and operated in such a way that users thereof may remain
anonymous if they so chose;
(c) if the system is used wholly or partly in connection with the business;
AND
(d) IF the system controller has made all reasonable efforts to inform [the
User] in advance … that the indirect communications transmitted by
means thereof may be intercepted or … with the express or implied
consent of the person who uses that telecommunications system

In other words – unless an employer has the employee’s written consent, the employer may
only lawful intercept communications in the course of transmission in limited circumstances.
The question is whether RIC Act would provide protection which regard to stored
communications (communications not in transit). The answer is possibly not.28 On a narrow
interpretation, employers (relying on s 6) may only intercept communications (without written
consent) while the communication is in the process of traversing the Internet or the
employer’s network. On a narrow reading, employers would need an employee’s consent to
access the employee’s communications on an information system. The critical issue therefore
is consent, and the various forms that such consent might take.

The ECT and RIC Acts, bounded by the employees’ constitutional right to privacy, may
restrict the control which an employer has over its resources such as its telephones and
computer systems.29 The matter of privacy in the workplace is likely to become even
more complicated with the enactment of the data protection principles and employers
are advised to seek upfront the necessary written consent to monitor from employees
but, even so, employers may be restricted in what they may legally process by way of
interception and monitoring, for privacy is a constitutional right, embodied in the data
protection principles.30

Employees and employers alike should be reminded that the extent of the right to
privacy may shrink as we move into the communal and business world,31 but that the
core of the fundamental right to privacy is likely to remain protected. What this means
in the workplace is an increasingly complicated matter.

28 A contrary view is suggested by Pistorius, T ‘Monitoring, Interception and big boss in the
workplace: is the devil in the details’ 2009 (1) PER 2-26 at 12.
29 The extent of the employer’s right to monitor and control the use of its communications
facilities arises most often in the context of the admissibility of evidence obtained by the
employer. The RIC Act does not expressly render information obtained in contravention of the
Act inadmissible in civil and criminal proceedings; and the prevailing view is that an employer
may use such evidence in disciplinary proceedings provided it is fair to do so. Grogan ‘Workplace
privacy’ (2004), Butterworths. This was the position prior to enactment of the RIC Act (Pretoria
Technology Ltd v Wainer 1997 (9) BCLR 1225 (W)). Fairness is determined on a case-by-case
basis with due regard to the extent of the measures (and their purpose) pursued by the
employer. In this regard see for example the standard-setting cases: Moonsamy v The Mailhouse
1999 (20) ILJ 464 (CCMA); Bamford & others v Energiser (SA) Limited [2001] 12 BALR 1251 (P);
30 It remains to be seen how the idea that privacy ‘requires a subjective expectation of privacy
which society recognizes as objectively reasonable’ (Pretoria Technology Ltd v Wainer 1997 (9)
BCLR 1225 (W)) will be interpreted in light of the plethora of privacy related legislation.
31 Bernstein v Bester NO 1996 (2) SA 751 (CC) at 789.
BIBLIOGRAPHY

Cases

_Bamford & others v Energiser (SA) Limited_ [2001] 12 BALR 1251 (P)

_Bernstein v Bester NO_ 1996 (2) SA 751 (CC)

_Moonsamy v The Mailhouse_ 1999 (20) ILJ 464 (CCMA)

_Pretoria Technology Ltd v Wainer_ 1997 (9) BCLR 1225 (W)


Statutes

Constitution of the Republic of South Africa

Electronic Communications and Transactions Act 25 of 2002

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Bill

Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002

Secondary Sources


Grogan, J 'Workplace privacy' (2004) Butterworths

Pistorius, T 'Monitoring, Interception and big boss in the workplace: is the devil in the details' 2009 (1) _PER_ 2-26


The Information Commissioner's Office 'Employment Practice Code'. Available at [www.ico.gov.uk](http://www.ico.gov.uk)