Chapter 39

Privacy

'Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.'

Edward Snowden (1983–)
former Central Intelligence Agency employee who copied and leaked classified information from the US National Security Agency in 2013 without prior authorisation

What is covered in this chapter

WHY THIS CHAPTER IS IMPORTANT

Some people may think privacy is not all that important, but just think what could happen to you if a criminal syndicate was able to hack access to your private details stored on your bank's computer network. If details of your full name, ID number and address were stolen, a dishonest person could falsify applications for a drivers' licence, passport, telephone, cellphone account, bank account, and credit card … all in your name … and you could land up paying the bills for whatever they do!

Privacy and protection of personal information is a developing area of our law. Criminal syndicates across the world are hacking into computer networks run by governments, banks and large companies to try to access the private information they hold. This is one of the reasons that consumers are asked regularly to change passwords, and to keep their private information secret. Microchip technology is being added to credit cards, and bank customers are being required to use their fingerprints when accessing their accounts. Identity theft and online fraud are very real problems with which businesses have to deal every day.

PRIVACY

1 Privacy and the Constitution

The right to privacy is recognised in the Bill of Rights in our Constitution.[1] This right provides that the privacy of communication may not be infringed unreasonably.

In common with all other rights in the Bill of Rights, the right to privacy is not absolute. This means that this right may be limited to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom. The limitation must take into account all relevant factors, including: the nature of the right; the importance of the purpose of the limitation; the nature and extent of the limitation; the relation between the limitation and its purpose; and whether there are less restrictive means that could be used instead, to achieve the same purpose.

***National Coalition for Gay and Lesbian Equality v Minister of Justice*[2]**

The Constitutional Court held that the concept of privacy recognises that we all have a right to a sphere of private intimacy and autonomy which allows us to establish and nurture human relationships without interference from the outside community.

***Olmstead v the United States*[3]**

In this well-known American case Justice Brandeiss described privacy as the 'right to be left alone – the most comprehensive of rights and the most valued by civilised men.' This view was endorsed by the Constitutional Court[4] when it held that privacy was 'an individual condition of life characterised by seclusion from the public and publicity. This implies an absence of acquaintance with the individual or his personal affairs.'

2 Privacy in employment[5]

Employers may require access to employees' private information for a variety of legitimate business reasons. These include:

- Assessment of applicants for prospective employment, including reference and criminal record checks, and medical examinations.
- Investigation of misconduct justifying disciplinary action.
- Assessment of performance and investigation of capacity.
- Control of absenteeism and sick leave: An employee who fails to report for work may be required to submit a medical certificate that must disclose the reason for the absence.
- Notification of contact people in cases of emergency.
- Tax purposes: Private information on earnings is disclosed to the State by the employer in compliance with relevant tax legislation.

1 Constitution of the Republic of South Africa, 1996.
2 *National Coalition for Gay and Lesbian Equality v Minister of Justice* 1999 (1) SA 6 (CC).
3 *Olmstead v the United States* 277 US 438 (1928) at 478.
4 *Bernstein and others v Bester and others* 1996 (4) BCLR 449 (CC).
5 Mischka, C, The Monitoring and Interception of Electronic Communications: Obtaining and Using E-mail and other electronic evidence, *Contemporary Labour Law*, Vol 10, May 2001; Mischka, C, Disciplinary Action and the Internet – Responding to Employee abuse of E-mail, Network and Internet Access, *Contemporary Labour Law*, Vol 9, 5 December 1999; McGregor, B, An analysis of e-communication in the workplace: The Risks and Solutions, *Seminar Paper*, Durban: Deneys Reitz (unpublished).

- Training in terms of compliance with the Skills Development Act.[6]
- Affirmative action compliance with the Employment Equity Act.[7] Information on race and gender is disclosed to the State when the employer submits its employment equity plan to the Department of Labour.
- Developing a scorecard to comply with Broad-Based Black Economic Empowerment.[8]
- Compliance with the Basic Conditions of Employment Act.[9]
- Collective bargaining: Wage levels, medical aid, sick pay funds, retirement, pension, and provident funds and membership of registered trade unions.

The employer's legitimate needs and requirements ought to be balanced against an employee's right to privacy. As a general principle, an employer's e-mail, internet and computer systems are normally used as business tools and are neither confidential nor private.

***Protea Technology Ltd and another v Wainer and others*[10]**

The company applied to court to enforce a restraint of trade clause in a contract of employment. The company relied on transcripts of tape recordings of telephone calls made by Mr Wainer whilst he was still in their employ. The recordings had been made secretly by means of a bugging device.

The court held that the Interception and Monitoring Prohibition Act[11] did not make information gathered in contravention of its provisions inadmissible in legal proceedings before a court trying a civil dispute. The court retained its common-law discretion to admit illegally obtained evidence, and held that such a discretion was reasonable in an open and democratic society.

On the argument by the employee that the transcripts were in breach of his constitutional right to privacy, the court held that the scope of a person's privacy extended only to those aspects in regard to which a legitimate expectation of privacy could be harboured. This legitimate expectation of privacy is a subjective expectation which society recognised as objectively reasonable. This in effect means the court will consider any claim to an expectation of privacy objectively and having regard to its reasonableness. Each case will accordingly be judged on its own merits.

The court found that there was no objectively reasonable expectation to privacy because of the following factors: the employee had been employed in a position of trust; the telephone conversations were conducted from the company's business premises within business hours; the telephone conversations of the employee relating to the employer's affairs were not private, and were accordingly not protected under the Constitution.

3 Legal consequence of unlawful invasion of privacy

Computers store information and the data is easily accessible. This allows for subtle, pervasive and intrusive forms of privacy invasion, in the collection, access, use and dissemination of personal information.

These may arise in a variety of forms:

6 Skills Development Act 97 of 1998.
7 Employment Equity Act 55 of 1998.
8 Broad-Based Black Economic Empowerment Act 53 of 2003.
9 Basic Conditions of Employment Act 75 of 1997.
10 *Protea Technology Ltd and another v Wainer and others* 1997 (9) BCLR 1225 (W).
11 Interception and Monitoring Prohibition Act 127 of 1992.

3.1 Common-law protection of privacy

Our courts have defined the right to privacy as 'the right to determine destiny of private facts and … includes the right to decide when and under what conditions private facts may be made public.'[12]

The common-law crime of *crimen injuria* has been developed by the courts in order to provide criminal protection of the right to privacy of information in the material world. *Crimen injuria* is defined as the wrongful, intentional and serious infringement of another person's dignity or privacy.[13]

The most common way in which *crimen injuria* can be committed where another person's privacy is invaded is where a person peeps into the window of an undressing man or woman.[14] Similarly, a person planting a listening device in order to eavesdrop on another person's private conversation is also guilty of *crimen injuria*.[15]

3.2 Legislative protections of privacy

3.2.1 Promotion of Access to Information Act[16]

Information held by the State or private bodies may be accessed, provided that it is required for the exercise or protection of any right. The definition of a 'private body' is very wide and includes any person or entity, including a partnership, that has ever carried on any business, trade or profession. Access to information may be limited for the reasonable protection of privacy, commercial confidentiality and effective, efficient and good governance.

A person who wants to request any record from a public or private body must:

- Provide sufficient particulars to enable the records requested and the requester to be identified.
- Indicate whether the record can be photocopied, transcribed, reproduced by equipment, or downloaded.
- State the language in which the information should be supplied.
- Provide a postal address or fax number.
- Provide contact details to be informed of the outcome of any request for information.
- Submit proof of the requester's capacity if the request is being made on behalf of another person.

The private body is allowed in certain circumstances to refuse. An applicant who is aggrieved by the refusal may apply to a court to determine whether the refusal is justifiable or not.

***Institute for Democracy in South Africa and others v African National Congress and others*[17]**

The applicant requested a political party to identify the sources of its funding.

The court held that the applicant failed to prove that it was entitled to information regarding certain donations that the ANC received. For purposes of its donations records, the ANC was held to be a private and not a public body. In receiving private donations, the ANC was not exercising any powers or performing any functions in terms of the Constitution; exercising a public power or performing a public function in terms of any legislation; or exercising any power or performing any function as a public body.

12 *National Media Ltd and another v Jooste* 1996 (3) SA 262 (A) at 271.
13 *Rex v Umfaan* 1908 TS 62.
14 *Rex v Holliday* 1927 CPD 395.
15 *S v A and another* 1971 (2) SA 293 (T).
16 Promotion of Access to Information Act 2 of 2000.
17 *Institute for Democracy in South Africa and others v African National Congress and others* 2005 (5) SA 39 (C).

Not all information is accessible in terms of the Act. Certain categories of documents and records are protected in the interests of privacy.

The categories of protected information include:

- Personal information about a third party, including a deceased individual.
- Records of the South African Revenue Service containing information which was obtained to enforce legislation concerning the collection of revenue in terms of the South African Revenue Service Act.[18]
- Trade secrets.
- Financial, commercial, scientific or technical information, the disclosure of which would be likely to cause harm to the commercial or financial interests of that third party.
- Information supplied in confidence, the disclosure of which could reasonably be expected to place that third party at a disadvantage in contractual or other negotiations or prejudice the third party in commercial competition.
- Information that, if released, would constitute an action for breach of a duty of confidence.
- Information that could reasonably be expected to endanger the life or physical safety of an individual or compromise the safety and security of any property.
- Records that contain information used for the purposes of law enforcement and legal proceedings.
- Information pertaining to the defence, security and international relations of the country.
- Information concerning the economic interests and financial welfare of the country.
- The commercial activities of public bodies.
- Research information of a third party or a public body.
- Information pertaining to the operations of public bodies.
- Medical information held by a health practitioner.

***Minister for Provincial and Local Government v Unrecognised Traditional Leaders, Limpopo Province (Sekhukhuneland)*[19]**

The court considered the refusal of the Premier of Limpopo to release a report investigating irregularities and malpractices in the appointment of traditional leaders. The Minister argued that the report was submitted to assist him to formulate a policy or to take a decision in the exercise of a power or performance of a duty, and that he was entitled to deny the Association's request for access in terms of the Promotion of Access to Information Act.[20]

The court held that because the purpose of the Act was to give effect to access to information and promote the values of openness, transparency and accountability that are fundamental to the Constitution, reliance on the Act to prohibit access to information should be limited, rather than expanded. The court ordered the Minister to allow the Association access to the report.

Despite the exceptions, information should be disclosed if it can be shown that there is either a substantial failure to comply with the law, or an imminent and serious public safety or environmental risk. It must also be shown that the public interest served in the disclosure of the record clearly outweighs the harm contemplated in the exclusion.

18 South African Revenue Service Act 34 of 1997.

19 *Minister for Provincial and Local Government v Unrecognised Traditional Leaders, Limpopo Province (Sekhukhuneland)* 2005 (2) SA 774 (SCA).

20 Promotion of Access to Information Act 2 of 2000.

Andrew Christopher Davis v Clutcho (Pty) Limited[21]

A dispute arose between family members who ran a company. The applicant wanted to sell his shares in the company, and wanted access to the financial books to find out the true financial position. The respondent refused because it said the records were highly relevant to the financial viability of the business and would provide the applicant with detailed insight into the business's customer lists, financial planning and profit margins. It was alleged that if the information was disclosed it would be likely to cause harm to the commercial and financial interests of the respondent.

The court held that it could never have been the intention of the legislature that a shareholder aggrieved by financial statements should be barred from access to information about these statements, so that he could exercise his rights to sell shares or even take legal action against the company in terms of the Companies Act[22] or the common law.

The court held that the respondent did not prove that its profit margins were trade secrets or that the requested disclosure was likely to cause harm to its commercial or financial interests. Accordingly, the court granted an order entitling the applicant to the information. However, he was not allowed access to customer lists, as the court decided that this was a justifiable limitation of his rights of access. Access to the information was also restricted to the applicant and his lawyer.

Provided there is no reason to refuse the information, access must be given to records of public bodies if the correct procedures are used. However, if it is a private body, the Act[23] imposes a further requirement before any information is released, namely, that the record must be 'required for the exercise or protection of any rights'.[24]

The meaning of 'required' has been interpreted by our courts to mean that it will be of assistance in the exercise or protection of the right. The applicant has to state what the right is that they wish to exercise or protect, what the information is which is required and how that information would assist in exercising or protecting that right.[25] Mere 'assistance' is not enough. Rather, the information must be 'reasonably' required. This conveys an element of need: the information does not have to be 'essential', but it certainly has to be more than 'useful' or 'relevant' or simply 'desired'.[26]

Unitas Hospital v Van Wyk[27]

An applicant requested disclosure of a report on nursing standards at a hospital. She wanted to use the report to help in developing a claim against the hospital.

The court held that the request for the record did not even meet the threshold test of 'assistance' because the author was one of the applicant's expert witnesses and could give the information to her; and the report was not directly causally linked to the care given to the late Van Wyk. Disclosure would only serve the purpose of embarrassing the hospital. She did not need the record to formulate her claim as she already had enough information to enable her experts to determine the merits of the matter.

The court stated that the requester must need the documentation for the exercise or protection of a right. It must be available only to a requester who has shown the 'element of need' or

21 *Andrew Christopher Davis v Clutcho (Pty) Limited* (1289/03) [2003] ZAWCHC 23 (10 June 2003).
22 Companies Act 61 of 1973.
23 Promotion of Access to Information Act 2 of 2000.
24 Wilson, M, Unitas Hospital v Van Wyk: The meaning of 'required' in s 50(1) of the Promotion of Access to Information Act 2 of 2000, *De Rebus*, Pretoria: Law Society of South Africa July 2006.
25 *Cape Metropolitan Council v Metro Inspection Services (Western Cape) CC and others* 2001 (3) SA 1013 (SCA).
26 *Clutchco (Pty) Ltd v Davis* 2005 (3) SA 486 (SCA).
27 *Unitas Hospital v Van Wyk* 2006 (4) SA 436 (SCA).

'substantial advantage'. The requester must need the record in order to formulate her claim for purposes of instituting an action. If she can commence her claim without it, then the element of need was not met. The requested record must therefore be essential or necessary for the exercise or protection of a right.[28]

Once the private body receives a request for access to certain records, it is obliged to take all reasonable steps to inform the person about whom the requested information or record relates. The person concerned may then either agree to the release of the information concerned, or object to the disclosure of the information.

***SA Metal and Machinery Co (Pty) Ltd v Transnet Ltd*[29]**

The applicant had tendered unsuccessfully for the purchase of scrap metal from the respondent. SA Metal then asked Transnet to provide documents showing the name and address of the successful tenderer and the price. Transnet refused, arguing it was allowed to withhold the information because its disclosure would be likely to cause harm to the commercial or financial interests of the other tenderers.

The court held that tender prices, where the tender date had already passed, were not the type of information for which disclosure may be justifiably refused. Any advantage a competitor might have gained in order to submit a better price was lost once the tender date had passed. Also, Transnet was not a third party and so could not rely on a part of the Act that allowed information to be withheld if its release would cause harm to a third party.

A private body must grant access to a record if the person requesting the information complies with the provisions of the Act. To facilitate access to records held by public and private bodies, the Act requires that the procedures to obtain those records must be in writing and made available to the public. All private bodies must compile a manual containing a description of all the documentary information held by it.

The manual must contain the following information:

- The full name, physical and postal addresses and contact details of the head of the private body.
- A description of the guide to be published by the Human Rights Commission in terms of section 10 of the Act.
- Categories of information readily available to the public from the private body without making a formal request for information.
- The manner in which a formal request for information should be lodged with the private body.
- The identity and contact details of any person duly authorised by the head of the private body to assist with or facilitate requests for information.
- The categories of information held by the private body, including the subjects on which the private body holds such information, which may be obtained only by means of a formal request for information.

The manual may include additional information to assist members of the public when making a request to a private body for information. This additional information may include:

28 Wilson, M, Unitas Hospital v Van Wyk: The meaning of 'required' in s 50(1) of the Promotion of Access to Information Act 2 of 2000, *De Rebus*, Pretoria: Law Society of South Africa July 2006.

29 *SA Metal and Machinery Co (Pty) Ltd v Transnet Ltd* [2003] 1 All SA 335 (W).

- The right of a requestor to appeal refusals by the head of a private body to grant a request for information, the manner in which information is to be provided by a private body and the time periods within which the information is to be made available.
- The grounds on which information may be refused.
- The rights of third parties regarding information that may concern those third parties.

Care should be taken to compile the manual in a manner that will promote access to information, rather than frustrating it.

A further measure to ensure the protection of personal information is the appointment in writing of someone who is responsible for protecting information within an organisation, and held accountable for any misuse of the data held. This person is known as the Information Officer, and is normally the head of the business unless the appointment is delegated to another employee at senior level within the same organisation. It is not possible for an external person to be appointed.

The Information Officer is the point of contact between the organisation and the Regulator. They provide education for employees on compliance requirements and training for staff responsible for processing personal information. The Information Officer must also conduct regular security audits and make recommendations to improve compliance with the Act and best practice.

An Information Officer who fails to adequately perform their duties may be held personally liable, with a fine of up to R3 000 per infringement.

3.2.2 The Regulation of Interception of Communications and Provision of Communication-related Information Act[30]

This Act regulates the extent to which individuals and corporations may lawfully intercept and monitor their employees' communications.

No person may intentionally intercept any 'communication' in the course of its occurrence or transmission, anywhere in South Africa. Anyone guilty of breaching the Act may face a fine of up to R2 million or up to ten years' imprisonment.

A 'communication' means both indirect and direct communications:

- **Indirect communication**: This means the transfer of information by a telecommunication system or a postal service. This includes speech, music or other sounds, data, text, visual images, signals or radio frequency spectrum. An indirect communication includes, for example, a telephone conversation, e-mail transmission, fax, SMS, postal communication and downloading information from the internet.
- **Direct communication**: This means either:
  - Oral communication between two or more persons which occurs in the immediate presence of all the persons participating in that communication.

30 Regulation of Interception of Communications and Provision of Communication-related Information Act 70 of 2002.

- An utterance by a person participating in an indirect communication, if the utterance is audible to another person who is in the immediate presence of the person participating in the indirect communication.

  A direct communication includes, for example, face-to-face discussions between two or more people, or a telephone conversation overheard by a third party who is present with one of the callers.

'Interception' means to acquire the contents of any communication through whatever means, so as to make some of the contents available to a person other than the sender or intended recipient. Interception includes monitoring by means of a monitoring device, viewing, examining or inspecting the contents of any indirect communication, and diverting any indirect communication from its intended destination.

The Interception Act provides three exceptions to the general prohibition on interception of a communication:

- If the interceptor is a party to the communication.
- If one of the parties to the communication has given their prior consent in writing to the interception.
- For lawful business. The lawfulness will depend on the nature and content of the intercepted communication; the purpose for which the interception is effected; the nature of the telecommunications system involved; and the measure of control exercised over the interception process by the system controller.

An employer may lawfully monitor, examine and otherwise intercept employees' telephone conversations, e-mails, faxes and other forms of indirect communication, in the course of the carrying on of its business provided that:

- The communication is the means through which a transaction is entered into in the course of that business.
- The communication is intercepted for a legitimate purpose. For example, to investigate or detect the unauthorised use of the employer's telecommunication system.
- The communication is intercepted over a telecommunication system that is provided for use in connection with the business of the employer.
- The system controller has made all reasonable efforts to inform all individuals using the telecommunication system in advance that indirect communications transmitted through it may be intercepted, and the system controller has intercepted the communication personally.

The business exception only applies to indirect communications transmitted over a telecommunication system as defined in the Telecommunications Act,[31] intercepted during the course of transmission. In terms of that Act, a telecommunications system is 'any system or series of telecommunications facilities or radio, optical or electromagnetic apparatus or any technical system used for the purpose of telecommunication, whether or not such telecommunication is subject to re-arrangement, composition or processes by any means in the course of the transmission or emission or reception'.

Face-to-face discussions and other forms of direct communication cannot lawfully be monitored on this basis. Nor can an employer intercept employees' post and other forms of indirect communication not transmitted over a telecommunications system. The business

31 Telecommunications Act 103 of 1996.

exception will not apply once an e-mail or other message or download arrives at its destination since the Interception Act makes it clear that interception must occur 'during the course of transmission'.

These provisions confirm that where a company's computer system is used as a business tool, an employer is entitled to monitor that such a tool is used for its benefit and is not abused. Even where monitoring has been in contravention of a statute, the employer has been able to rely on such evidence to justify the dismissal of employees engaged in the abuse of the employer's computer system.[32]

Because of the wide range of communications that fall outside the ambit of the business exception, it remains important for an employer to obtain correctly worded written consent in advance from employees. For example, if an employer deems it necessary to monitor what an employee has downloaded and saved to their computer, the employee would have to provide prior written consent.

Interceptions are allowed in the course of the carrying on of an employer's business. These are meant to allow for businesses to prevent the misuse of telephones, e-mail and the internet, as well as to protect business systems against viruses, hackers and similar threats.

Legitimate reasons for intercepting indirect communications could therefore include the purpose of detecting hardware and software problems or errors, monitoring for viruses, attempts at hacking and other threats to the system, automated processes such as caching or load distribution, and ensuring compliance with software-licence agreements.

3.2.3 The Electronic Communications and Transactions Act[33]

The Act protects personal information by providing a set of principles to which data controllers may voluntarily subscribe. Any data controller who intends to subscribe to the voluntary code must subscribe to all the principles, and not just to parts of the code.

The code provides that a data controller must:

- Obtain permission to record personal information.
- Disclose the purpose for which they seek the information.
- Not collect information which is irrelevant to the data subject.
- Refrain from using the information for any other purpose.
- Keep a record of at least one year after collection of what the information was and the purpose for which it was collected.
- Not disclose the information without permission.
- Destroy all such information when it becomes obsolete.

The Act gives the State a right to declare certain databases critical in the interests of national security or for the purposes of the economic and social well-being of South Africans. If this is done, the controller of the database must disclose certain information in respect of the database and must conform to database-management standards stipulated by the State.[34]

The Act creates a cyber inspectorate, a government watchdog force that ensures compliance with the Act and monitors cyber crimes. Cyber inspectors are granted reasonably extensive powers in the monitoring of web pages, public information systems, cryptography service providers, authentification service providers, and electronic transactions.

---

32 *Tap Wine Trading CC v Cape Classic Wines (Western Cape) CC* 1994 (4) SA 194 (C); *Protea Technology Ltd and another v Wainer and others* 1997 (9) BCLR 1225 (W); *S v Kidson* 1999 (1) SACR 338 (W); *S v Dube* 2000 (2) SA 583 (NPD).

33 Electronic Communications and Transactions Act 25 of 2002; Stassen, P and K, New Legislation, *De Rebus*, Pretoria: Law Society of South Africa November 2002.

34 E-Commerce, *Business and Investment in South Africa*, Sandton: Cliff Dekker Attorneys, May 2005.

Activities that are aimed at preventing interference with commercial activities are 'cyber crimes'. These crimes include 'hacking', which is the unauthorised access to, and tampering with, data messages, and also computer-related extortion, fraud and forgery.

The Act also addresses the issue of 'spam' or junk mail distributed electronically. Anyone who forwards, by electronic means, an unsolicited commercial communication to potential consumers must disclose the source from which the recipient's contact details were obtained and also give the recipient the opportunity to refuse to receive any further communications from that source. It is a criminal offence in terms of the Act to fail to comply with these duties.[35]

A person who intentionally accesses or intercepts any data without authority or permission is guilty of an offence. The penalty is a fine or imprisonment for up to 12 months.

4 The Protection of Personal Information Act[36]

The Protection of Personal Information Act[37] aims to regulate every step of data processing of personal information, from collection to destruction. It also seeks to bring South Africa in line with global legislation regulating personal information. By doing this it facilitates international trade.[38]

4.1 Application of the Act

The Act applies to 'responsible parties', which are any public or private body or any other person who uses or processes 'personal information'. This is information relating to an identifiable, living, natural or juristic person (the 'data subject').[39]

'Personal information' includes:

- 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.
- Information relating to the education or the medical, financial, criminal or employment history of the person.
- Any identifying number, symbol, e-mail address, physical address, telephone number or other particular assignment to the person.
- The blood type or any other biometric information of the person.
- The personal opinions, views or preferences of the person.
- 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.
- The views or opinions of another individual about the person.
- 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.

35 E-Commerce, *Business and Investment in South Africa*, Sandton: Cliff Dekker Attorneys, May 2005.

36 Protection of Personal Information Act 4 of 2013.

37 Ibid.

38 KPMG South Africa Information Manual, Cape Town: KPMG, June 2021, available at https://home.kpmg/za/en/home/insights/2021/07/kpmg-south-africa-information-manual.html, accessed 20 December 2021.

39 Milo, D, *Protection of Personal Information Bill*, Johannesburg: Webber Wentzel 2011, as cited in *Creamer Media Reporter*, Protection of Personal Information Bill. Available at http://www.polity.org.za/article/protection-of-personal-information-bill-2009-10-21, accessed 23 December 2011.

The Act separates 'special personal information' from 'personal information'. Special personal information is information concerning a child who is subject to parental control in terms of the law; or a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life, or criminal behaviour. Subject to certain exclusions, the processing of special personal information is generally prohibited.[40]

The Act does not apply to the following situations:[41]

- Where informed consent is given voluntarily.
- For journalistic, literary or artistic expression (but only to the extent necessary to reconcile the right to privacy with the right to freedom of expression).
- To process personal information for any of the following purposes:
  - Purely personal or household activity.
  - Where the information is made anonymous.
  - For a public body involving national security or the prevention of unlawful activities (but only to the extent that adequate safeguards have been established in legislation).
  - By the cabinet or the executive council of a province.
  - Relating to the judicial functions of a court.

In addition, the processing of certain information is exempt from the Act when done to protect members of the public against financial loss due to improper conduct, unfitness or incompetence of any of the following:

- Persons authorised to carry on any profession or other activity.
- Persons who provide banking, insurance, investment or other financial services.
- Persons who manage bodies corporate.

The Regulator may grant an exemption to one or more conditions applicable to processing information if it is in the public interest, or where the processing involves a clear benefit to the data subject or a third party.

4.2 The information-protection principles

The Act sets out eight information-protection principles that must be complied with by a responsible party who processes personal information. These principles are regarded internationally as an acceptable compromise between the legitimate need to use personal information for business purposes, and the duty to provide access to information.[42]

4.2.1 Principle 1: Accountability

Responsible parties must assign responsibility for overseeing compliance with the Act. The person assigned will be known as the Information Protection Officer (IPO). It is this person's role to encourage and support the responsible party's overall compliance with the legislation.

40 When is the further processing of personal information applicable? POPI Bumper Special Alert, Johannesburg: Cliff Dekker Hofmeyr 30 June 2020. Available at https://www.cliffedekkerhofmeyr.com/export/sites/cdh/en/news/publications/2020/corporate/Downloads/POPI-Bumper-Special-Alert-30-June-2020.pdf, accessed 20 December 2021.

41 Moorcroft, J, POPI and the legal profession: What should you know? *De Rebus*, Pretoria: Law Society of South Africa October 2016.

42 KPMG South Africa Information Manual, Cape Town: KPMG, June 2021, available at https://home.kpmg/za/en/home/insights/2021/07/kpmg-south-africa-information-manual.html, accessed 20 December 2021.

The responsibilities of the IPO include monitoring the responsible party's compliance with the legislation and submitting reports to the Regulator. The IPO must also develop a data-protection policy setting out the organisation's approach to personal data processing. All employees should be trained in their duties in respect of personal data processing as well as the consequences of non-compliance.

4.2.2 Principle 2: Limiting the scope of processing

Personal information may only be processed in a fair and lawful manner so as not to intrude upon the data subject's privacy to an unreasonable extent.

The definition of processing is not limited to electronic personal information but includes paper-based records. In addition, processing includes various activities including collection, storage, use, display, transfer, archiving, modifying, maintaining and destruction.

Only the minimum amount of personal information may be processed to achieve the purpose for which it is required. The express consent of the individual must be obtained before the processing of personal information.

4.2.3 Principle 3: Purpose specification

Responsible parties must define the scope within which personal information may be processed.

A responsible party must ensure that personal information is only processed for specific, explicitly defined and legitimate reasons relating to the functions or activities of the organisation.

The responsible party must take steps to make the data subject (person whose personal information is being processed) aware of the purposes for which the personal information will be processed, as well as the intended recipients of the information. It must also establish mechanisms to ensure that personal information is only kept for as long as it is required to fulfil the purpose for which it was collected.

4.2.4 Principle 4: Further processing limitation

Responsible parties may only use personal information for purposes that were specified at the time that the individual consented to the processing of the information. If personal information is to be used for any other purpose or disclosed to any other recipients, the further consent of the individual must be obtained.

4.2.5 Principle 5: Information quality

Responsible parties are responsible to ensure and maintain the quality of the personal information that they process. They must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

4.2.6 Principle 6: Openness

Responsible parties have a duty to process information in a fair and transparent manner. For processing to be fair, individuals must be aware that their specific personal information is being held by particular responsible parties. Personal information may only be processed by a responsible party that has notified the Information Protection Regulator.

The responsible party must take reasonably practicable steps to ensure that the data subject is notified of all the following: that personal information is being collected; the name and address of the organisation; the purpose for which the information is being collected;

whether or not the supply of the information by that individual is voluntary or mandatory; the consequences of the failure to provide the information; any particular law authorising or requiring the collection of the information; information regarding the recipients or category of recipients of the information; and the existence of the rights of access to and rectification of the information being collected.

4.2.7 Principle 7: Security safeguards

All personal information should be kept secure against the risk of loss, unauthorised access, interference, modification, destruction or disclosure.

There is a general duty on a responsible party to secure the integrity of the personal information under its control. This means that the responsible party must ensure that personal information is protected against the risk of unauthorised access, modification or loss. The fact that personal information may be processed by a third party does not absolve the responsible party of its obligations as the party responsible for compliance with the law.

The third party may not process personal information on behalf of the responsible party without the knowledge and authorisation of that responsible party. The responsible party must ensure that the third party implements the security measures required. There must be a written contract in place between the responsible party and the third party which requires the third party to maintain the confidentiality and integrity of personal information processed on behalf of the responsible party.

If the third party is located outside of South Africa, the responsible party must ensure that the third party complies with any foreign laws relating to personal information applicable to the third party.

If personal information has been compromised, or if there is a reasonable belief that a compromise has occurred, the responsible party must notify the Regulator and the affected individuals in writing of the compromise as soon as reasonably possible.

4.2.8 Principle 8: Data subject participation

Individuals may access or request the correction or deletion of any personal information held about them that may be inaccurate, misleading or outdated.[43]

An individual may make two types of requests: confirmation of whether a responsible party holds any personal information about them (free of charge); or a description of the personal information held about them, including details of any third parties that may have access to that information (for a reasonable fee).

The responsible party must respond to the request for information within a reasonable period of time.

When responding to a request for personal information, the responsible party must inform the individual of the additional right to request the following:

- Correction or deletion of information that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; and
- Destruction or deletion of a record containing personal information that the responsible party is no longer authorised to keep or that is no longer necessary for the purpose for which the information was obtained.

43 Milo, D, *Protection of Personal Information Bill*, Johannesburg: Webber Wentzel 2011, as cited in *Creamer Media Reporter*, Protection of Personal Information Bill. Available at http://www.polity.org.za/article/protection-of-personal-information-bill-2009-10-21, accessed 23 December 2011.

The responsible party must provide credible proof to the individual of the action that has been taken in response to the request. If any changes to the personal information will have an impact on any decisions to be made about the individual, the responsible party must inform all third parties to whom the information has been disclosed of such changes.[44]

4.3 Rights of the data subject

The data subject has the right to object to the processing of personal information, and to request details of any personal information held about them, and information about any third parties who have or have had access to that information, as well as the right to correct or have deleted certain personal information.[45]

Personal information that is processed in a fully or partly automated manner may only be processed if the responsible party has notified the Regulator in the prescribed manner, in advance. Failure to notify is an offence.

The Regulator may authorise the processing of information that is in breach of the Act in certain circumstances such as where public interest in the processing of the personal information substantially outweighs any resultant interference with the data subject's right to privacy.

The processing of personal information for the purpose of direct marketing by means of automatic calling machines, SMSs or electronic mail is prohibited unless the data subject has given consent to the processing; or the data subject is a customer of the responsible party and has provided consent.

Any direct marketing, including spam, must contain details of the identity of the sender or the person on whose behalf the communication has been sent; and an address or other contact details to which the recipient may send a request that such communications cease.

4.4 Enforcement and penalties

Any person may lodge a complaint with the Regulator in certain circumstances, including for a breach of the principles or the provisions relating to unsolicited communications, directories and automated decision making. The Regulator has extensive powers of investigation including the right to apply to court for a warrant to enter and search premises. Data subjects, or the Regulator on their behalf, may also bring a claim for damages in certain circumstances, irrespective of whether there is intent or negligence involved.[46]

Contravention of any of the Principles is not a criminal offence. However the Regulator may issue an enforcement notice for a breach of the Act, and failure to comply with an enforcement notice is a criminal offence. On conviction a person may be liable to a fine and up to 12 months' imprisonment. If the offence relates to obstructing the Regulator the person is liable to a fine and up to ten years' imprisonment.

44 Milo, D, *Protection of Personal Information Bill*, Johannesburg: Webber Wentzel 2011, as cited in *Creamer Media Reporter*, Protection of Personal Information Bill. Available at http://www.polity.org.za/article/protection-of-personal-information-bill-2009-10-21, accessed 23 December 2011.

45 Ibid.

46 Ibid.

THIS CHAPTER IN ESSENCE

1 In common with all other rights in the Bill of Rights, the right to privacy is not absolute but may be limited to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom.
2 Employers may require access to employees' private information for a variety of legitimate business reasons. As a general principle, an employer's e-mail, internet and computer systems are normally used as business tools and are neither confidential nor private.
3 *Crimen injuria* is a common-law crime defined as the wrongful, intentional and serious infringement of another person's dignity or privacy.
4 Under the Promotion of Access to Information Act, information held by the State or private bodies may be accessed, provided that it is required for the exercise or protection of any right. Access to information may be limited for the reasonable protection of privacy, commercial confidentiality and effective, efficient and good governance. Procedures to obtain those records must be in writing and made available to the public.
5 The Regulation of Interception of Communications and Provision of Communication-related Information Act regulates the extent to which individuals and corporations may lawfully intercept and monitor their employees' communications. Interceptions are allowed in the course of the carrying on of an employer's business.
6 The Electronic Communications and Transactions Act provides a set of principles to which data controllers may voluntarily subscribe. Activities that are aimed at preventing interference with commercial activities are cyber crimes, which include hacking, computer-related extortion, fraud and forgery. The Act also addresses the issue of spam or junk mail distributed electronically.
7 The Protection of Personal Information Bill aims to regulate every step of data processing relating to personal information from collection to destruction. The bill sets out eight information-protection principles that must be complied with by a responsible party who processes personal information.