Chapter 8
Protection of data privacy in South African positive law

Contents

1 INTRODUCTION

In the previous chapter the dogmatic foundations of the legal protection of the data subject in the South African law of delict were examined. In this chapter, the subject investigated is the extent to which the protection of the data subject that is theoretically possible in our law has in fact been realised in positive law. In other words, the aim is to establish to what extent the data protection principles have been implemented in South African positive law, either in case law or in legislation. The influence of the

Constitution in this regard will also be discussed.

2 RECOGNITION OF DATA PRIVACY IN CASE LAW

In South African case law the concept of "data protection" or "data privacy" has not been identified and discussed as such. One case that does provide some idea of how South African courts might deal with data privacy in future is the criminal law case of *S v Bailey*.[1]

In this case the compulsory furnishing of information to the state in terms of the Statistics Act 66 of 1976[2] was at issue. The appellant, a medical practitioner, had been charged with a contravention of certain regulations promulgated under the Statistics Act, because he had failed to submit the census particulars and information required from medical practitioners by the regulations. He pleaded not guilty, his defence being that he was a private practitioner and he *bona fide* believed that he enjoyed a right of privacy that entitled him to refuse to complete the questionnaire. This, he contended, was a reasonable cause for noncompliance.

The court did not agree with his contention. The court held that the interference with plaintiff's right to privacy was lawful, because it was justified by "some superior legal right", namely the Statistics Act.[3] The question "is whether, when properly construed the Act and regulations authorise the interference complained of".[4] The court found that the Act and regulations were clear and without ambiguity and were expressed in peremptory language. The Act and regulations did not admit of any exceptions. A medical practitioner who considered that the information sought was private was not entitled to withhold the information on that ground alone.[5] Although the court had a measure of sympathy for the appellant

1 1981 4 SA 187 (N).

2 Replaced by the Statistics Act 6 of 1999.

3 *S v Bailey* 1981 4 SA 187 (N) 189.

4 *S v Bailey* 1981 4 SA 187 (N) 198.

5 *S v Bailey* 1981 4 SA 187 (N) 190.

who was required to furnish "an incredible mass of detail ranging across a very broad spectrum",[6] the court also assumed that "this information is reasonably required for the benefit of the community at large, is furnished with sufficient accuracy to be of some use, and that the whole thing is not simply an unnecessary exercise conducted by some self-promoting bureaucrats trying to justify their existence".[7]

The following principles can be deduced from the *Bailey* case with regard to the collection of personal information by the state:

- The collection of personal information is *prima facie* unlawful.[8]
- The existence of a ground of justification, such as statutory authority, may rebut *prima facie* wrongfulness.[9]

In future, any legislation that infringes the fundamentally recognised right to privacy will have to be tested against the Constitution,[10] and if such invasion is considered to be unreasonable and not justifiable, the legislation can be set aside.[11]

The permissible limitations of the constitutional privacy right were discussed in *Mistry v Interim Medical and Dental Council of South Africa*.[12] In this case information was communicated by one medicines control inspector to another for purposes of planning and implementing a search of premises

6 *S v Bailey* 1981 4 SA 187 (N) 190.

7 *S v Bailey* 1981 4 SA 187 (N) 190.

8 See also Neethling *Persoonlikheidsreg* 326 fn 49.

9 See ch 7 par 2.3.2.3.b.iv for a discussion of the ground of justification "statutory authority, official capacity and public interest".

10 See the limitation clause (s 36 of the Constitution) See ch 7 par 2.3.2.1.a.iv.

11 In *Bernstein v Bester NO* 1996 2 SA 751 (CC) the Constitutional Court held that the constitutionality of ss 417 and 418 of the Companies Act 61 of 1973 (requiring company directors or officers to provide information at meetings of creditors in company liquidation and insolvency hearings) should be assessed in the light of the control that the Supreme Court exercises over their implementation and as such they are consistent with the right to privacy protected by s 13 of the Interim Constitution, 1993.

12 1998 4 SA 1127 (CC) 1145.

in order to carry out a regulatory inspection. It was argued that this was an invasion of privacy as protected by section 13 of the interim Constitution and contrary to the secrecy provisions of the Medicines and Related Substances Control Act[13] and the Medical, Dental and Supplementary Health Services Professions Act.[14]

The Constitutional Court assumed for purposes of the decision that "informational privacy" was protected by section 13 of the interim Constitution.[15] The court held that the protection afforded by the right to privacy may be limited when a person's activities potentially pose a danger to the public and reasonable regulation of these activities therefore becomes necessary.[16] In finding that the applicant's constitutional right to informational privacy had not been breached,[17] the Constitutional Court held that a number of factors were important when considering whether a violation of the informational aspect of the right to privacy has taken place. These were:[18]

- whether information had been obtained in an intrusive manner (*in casu* it was volunteered by the public)

13 Act 101 of 1965 s 34.

14 Act 56 of 1974 s 41A(9)(a).

15 Act 200 of 1993. The court pointed out that informational privacy, unlike invasions of private communications, was not dealt with expressly by s 13. However, see Du Plessis & De Ville "Personal rights" 251 who argued that the term "personal privacy" in s 13 could be interpreted as referring to informational privacy rights.

16 *Mistry v Interim Medical and Dental Council of South Africa* 1998 4 SA 1127 (CC) 1145. According to McQuoid-Mason "Constitutional privacy" 18–2, if information is conveyed in circumstances analogous to a privileged occasion under common law, such disclosure may not necessarily be a breach of constitutional privacy, provided the information itself was not originally obtained as a result of such a breach. Also see Currie & Klaaren *AIA commentary* 117 (par 8.2).

17 However, s 28(1) of the Medicines and Related Substances Control Act 101 of 1965 which empowers inspectors to enter and search premises without a warrant and to seize and remove medicines from those premises, was found to be inconsistent with s 13 of the Interim Constitution. See further McQuoid-Mason "Constitutional privacy" 18–4. See also *Park-Ross v Director, Office for Serious Economic Offences* 1995 2 SA 148 (C) deciding that s 6 of the Investigation of Serious Economic Offences Act 117 of 1991 authorising the entry and search of premises without a warrant, was unconstitutional. For discussions of this case, see Kemp 2000 *Stell LR* 437, 445; Itzikowitz 1996 *THRHR* 497.

18 *Mistry v Interim Medical and Dental Council of South Africa* 1998 4 SA 1127 (CC) 1155–1156. See further Currie & Klaaren *AIA commentary* 117 (par 8.2).

- ❒ whether it was about intimate aspects of the applicant's personal life (*in casu* it was not – it was about how the applicant conducted his medical practice)
- ❒ whether it involved data provided by the applicant for one purpose which was then used for another (*in casu* it did not)
- ❒ whether it was disseminated to the press or the general public or to persons from whom the applicant could reasonably expect that such private information would be withheld (*in casu* it was communicated only to a person who had statutory responsibilities for carrying out regulatory inspections for the purpose of protecting public health and who was himself subject to the requirements of confidentiality)

3 CONSTITUTIONAL RIGHT OF ACCESS TO INFORMATION

One of the data protection principles is that data subjects must have a right of access to information collected on them.[19] Section 32(1) of the Constitution provides individuals with a right of access to information held by the state, or by another person in which case the information should be required for the exercise or protection of any rights.[20] This provision also enables the individual to gain access to his or her personal information and is thus also of importance for data protection. Section 32(2) of the Constitution furthermore provides that national legislation should be enacted to give effect to this right.[21]

---

19 See ch 6 par 2.2.

20 The section "favours a presumption of access to information in relation to state actors, whereas no such presumption exists in respect of private actors" (Pimstone 1999 *SAJHR* 2, 5).The requirement in the case of private bodies that there should be an antecedent right, has been interpreted to go beyond a right which arises in the course of formal action through the courts or which is contained in the Bill of Rights (*Qozeleni v Minister of Law and Order* 1994 3 SA 625 (E); *Van Huysteen NO v Minister for Environmental Affairs and Tourism* 1996 1 SA 283 (C) and *NISEC (Edms) Bpk v Western Cape Provincial Tender Board* 1998 3 SA 228 (C)). See further Pimstone 1999 *SAJHR* 2, 10 *et seq*; De Vos 1995 *Stell LR* 34, 50.

21 Section 32 of the Constitution, 1996 provides:

(1) Everyone has the right of access to
  (a) any information held by the state; and
  (b) any information that is held by another person and that is required for the exercise or protection of any rights.

(2) National legislation must be enacted to give effect to this right, and may provide for reasonable measures to alleviate the administrative and financial burden on the state.

(continued...)

The fact that a person has access to his or her personal information thus provides a connection between the right to privacy and section 32. According to Currie and Klaaren,[22] section 32 "gives legal recognition to the claim that the collection and dissemination of personal information by both public and private entities should be restricted". They argue that "at this level, freedom of information is closely connected to and overlaps with the right to privacy".

Eiselen[23] also emphasises the connection between access to information and data protection. He points out that the constitutional right of access to information strengthens the individual's position because the individual gets a right of access to information that involves his or her rights and this would definitely include personal information. Through this right of access to the information the individual gains a measure of control over the information.

4 PROTECTION OF DATA PRIVACY BY MEANS OF LEGISLATION

4.1 Introduction

At present there is no general data protection legislation in place. There is a growing awareness that personal information processed by third parties deserves special protection and legislation to deal with this issue is under consideration.[24] The following legislative measures, all of which contain certain data protection measures, merit discussion: The Promotion of Access to Information Act,[25] the Open

21(...continued)
The Promotion of Access to Information Act 2 of 2000 gives effect to this constitutional right. See par 4.2 below.

22 Currie & Klaaren *AIA commentary* 18 (par 2.5).

23 Eiselen *Reg op privaatheid in die inligtingsera* par 5.1.

24 In 2001 the South African Law Commission has appointed a project committee for Project 124 to consider privacy and data protection legislation.

25 Act 2 of 2000. For discussions of aspects of this Act, see Burns *Communications law* 101–104; Gaum2001 *THRHR* 146, 151–155; Naidoo 2001 (Feb) *De Rebus* 14–16; Stassen & Stassen 2001 (Jun) *De Rebus* 49–50; Visser 2002 *THRHR* 254–259.

Democracy Bill[26] and the Electronic Communications and Transactions Act.[27]

4.2 Promotion of Access to Information Act

4.2.1 Legislative history

As stated above, the Constitution enshrines the right of everyone to have access to information held by the state, or by another person, where such information is required for the exercise or protection of any rights;[28] it also provides that national legislation should be enacted to give effect to this right.[29] This was done in the Promotion of Access to Information Act (AIA)[30] which provides persons with a right of access to records of public bodies[31] and private bodies.[32]

This AIA was preceded by the Open Democracy Bill (ODB),[33] which contained not only provisions

26 B 67–98.

27 Act 25 of 2002. Also noteworthy is the Credit Bureaus Association's (CBA) code of conduct drawn up by the CBA. This code is a self-regulatory code that applies to all credit bureaus in South Africa. It was formally recognised by the Department of Trade and Industry in 1994. In brief, the code provides consumers with the opportunity to access information kept on them and to request a correction of inaccurate information. Provision is also made for the handling of disputes between credit bureaus and consumers. Furthermore, credit bureaus have a duty to treat subscribers and consumers as fairly and impartially as possible. They may only contract with subscribers who have a *bona fide* risk management reason for accessing the information. The subscribers must agree not to disseminate the information to any person other than the consumer concerned. Credit bureaus must follow reasonable procedures to ensure that the information they obtain is accurate, relevant and unbiased, and must keep a record of the source of information received and the subscribers who access the information. Only information relating to credit and business dealings may be recorded by bureaus.

28 Act 108 of 1996 s 32(1).

29 Act 108 of 1996 s 32(2).

30 Act 2 of 2000. The AIA was passed by parliament in January 2000 and assented to by the President on 2 February 2000. Regulations made by the Minister of Justice and Constitutional Development were published on 9 March 2001.

31 Act 2 of 2000 s 11.

32 Act 2 of 2000 s 50.

33 B 67–98.

regulating access to information, but also provisions regulating data privacy or data protection.[34] These provisions have been omitted from the AIA. There are two reasons for this: First, the time constraints on getting the AIA published before the constitutional deadline – only the access to information provisions were constitutionally required, and it was therefore possible to leave out any "unnecessary" parts of the Act in order to speed up its adoption and the framing of the accompanying regulations.[35] The second reason is that the *Ad Hoc* Committee on the ODB (that introduced the Bill to Parliament) felt that if the Act were to regulate certain aspects of the right to privacy, such as the correction of and control over personal information, it would be dealing with the constitutional right to privacy in "an *ad hoc* and undesirable manner".[36] The Committee was also of the opinion that South-Africa should enact separate privacy legislation, following the international trend.[37] Legislation based on the omitted provisions is therefore expected to follow.[38] Consequently, the data protection provisions of the ODB remain of interest and will be discussed below.

4.2.2 Objects of AIA

Section 9(a) of the Act makes it clear that one of its objects is to give effect to the constitutional right

34 Before the ODB was published, a draft Bill was published for comments (*GG* 18381 of 18–10–1997). The draft Bill was based on policy proposals made by the Task Group on Open Democracy. The recommendations of the Task Group were that an Open Democracy Act should have more than one function, including a freedom of information component, a privacy component, an open meetings component and a component protecting whistle blowers (see Williams 1997 (Aug) *De Rebus* 563, 565; Roos 1998 *THRHR* 497). The open meetings component was subsequently deleted and the Bill itself was further scaled down – only the access to information component remained in the AIA. The whistle blowers chapter of the ODB became the Protected Disclosures Act 26 of 2000. For a discussion of the history of the ODB and the differences between the draft Bill and the Bill subsequently approved by the cabinet, see White 1998 *SAJHR* 65. Also see Currie & Klaaren *AIA commentary* 2 *et seq* (par 1.2).

35 Joint Committee on Open Democracy Bill *Report* 17.

36 Joint Committee on Open Democracy Bill *Report* 17.

37 The Committee requested the Minister for Justice and Constitutional Development to introduce privacy and data protection legislation, "after thorough research on the matter, as soon as reasonably possible" (Joint Committee on Open Democracy Bill *Report* 17). See also Roos "Data protection" 43 and Klaaren, Currie & Smith "Access to information legislation" 31.

38 The Act itself also contains indications that further legislation is envisaged (see eg Act 2 of 2000 s 86 and s 88).

of access to information in section 32 of the Constitution.[39] However, according to section 9(b), effect will be given to this right subject to justifiable limitations, including limitations aimed at the reasonable protection of privacy, commercial confidentiality and effective, efficient and good governance. The AIA is therefore both legislation giving effect to the constitutional right of access to information and a law of general application limiting such right in the interests of specific other interests.[40]

Although the AIA is primarily a freedom of information act, the link between privacy and access to information is thus explicitly recognised in s 9(b), which justifies the Act's limitation of this constitutional right *inter alia* by "the reasonable protection of privacy".[41]

4.2.3 AIA and data protection

Not all the provisions of the AIA are of importance from the point of view of data protection.[42] The AIA promotes data protection by permitting individuals access to their own personal information and prohibiting access to third party information if this would lead to unreasonable infringement of the privacy of the third party. The Act also contains provisions regarding the correction of personal information as a transitional measure until a data protection act has been adopted, and provides for exceptions to the right to access personal information.[43]

---

39 The term "give effect to" is synonymous with "elaborate upon", "make effective" or "promote" (Currie & Klaaren *AIA commentary* 13 (par 2.1)). According to Currie & Klaaren *AIA commentary* 12 (par 2.1), the AIA has something of a dual character, because "it is at the same time a statute (an embodiment of the legislative will) and a legislative interpretation and supplementation of a constitutional provision (a set of values that stand above the will of the legislature). Both the Act's existence and, to a degree, its content are mandated by the Constitution to give effect to constitutional rights". It shares this status with the Promotion of Administrative Justice Act 3 of 2000, enacted to give effect to the rights of just administrative action in s 33 of the Constitution.

40 Currie & Klaaren *AIA commentary* 16 (par 2.4); Klaaren, Currie & Smith "Access to information legislation" 31.

41 Currie & Klaaren *AIA commentary* 18 (par 2.5).

42 The discussion of the AIA will focus on those provisions that are relevant for data protection.

43 See ch 6 par 2.2.8.

4.2.3.1 Access to information

The AIA permits individuals access to records containing personal information about themselves.[44] This is a reflection of the data protection principle that requires that data subjects should have a right of access to their personal information.[45]

The AIA provides for grounds on which a request for access must or may be refused.[46] Currie and Klaaren are of the opinion that very few of these grounds are sufficient to justify refusal to disclose personal information on the requester of such information. They give section 44(2)(b) as an example, which permits refusal of disclosure of confidential evaluative material about a requester.[47] Other examples which could probably also justify refusal to disclose personal information on the requester are section 38(a), which mandates refusal for the protection of the safety of individuals, section 39 which mandates protection of police dockets in bail proceedings and the protection of law enforcement and legal proceedings; section 40 which mandates protection of records subject to privilege in legal proceedings; and section 41 which permits refusal of access in the interests of the defence, security and international relations of the Republic.[48]

It is possible that the AIA might ultimately be the only legislation in terms of which access to information can be requested, even if separate privacy or data protection legislation is adopted. If the legislature decides to regulate all instances of access to information in a uniform manner, it need not include access

---

44 Act 2 of 2000 s 11 and s 50, read with the definition of "personal requester" in s 1.

45 Currie & Klaaren *AIA commentary* 120 (par 8.6) fn 17 describe this as the "informational self-determination" aspects of the right to privacy. This term was used by the German constitutional court in the 1983 "Census decision" (see ch 2 fn 113). Also see Burkert "Data protection and access to data" 50 for an essay on the differences between data protection and access to (government) information legislation.

46 Act 2 of 2000 s 33–44; s 62–69.

47 Currie & Klaaren *AIA commentary* 120 (par 8.6). On this ground of refusal, see par 4.2.7.3.

48 See par 4.2.7.3.

to information provisions in subsequent data protection legislation.[49] The Electronic Communications and Transactions Act[50] does not, for example, contain any access to information provisions because this aspect is taken care of in the AIA. The access provisions of the AIA will therefore be dealt with in detail.

4.2.3.2 Mandatory protection of privacy of third party

The right of access to information is not intended to be used to obtain personal information about other individuals that would result in an infringement of their right to privacy.[51] Sections 34[52] and 63[53] of the AIA therefore provide for mandatory protection of a third party (who must be a natural person according to the headers of the sections) by providing that a public or private body must refuse a request for access to a record if its disclosure would involve unreasonable disclosure of personal information about a third party.[54] This ground of refusal will be discussed in more detail below.[55]

4.2.3.3 Correction of personal information

The AIA provides that if no provision for the correction of personal information in a record held by a public or private body exists, that body must take "reasonable steps" to establish "adequate and

49 At present the National Environmental Management Act 107 of 1998 is the only piece of legislation specifically permitted by the AIA to regulate a supplementary but separate access to information scheme (see par 4.2.4.1).

50 Act 25 of 2002.

51 See eg *Water Engineering & Construction (Pty) Ltd v Lekoa Vaal Metropolitan Council* [1999] 2 All SA 600 (W) 605 where Epstein AJ held: "In my view, it cannot be that unrestricted access was intended by the framers of the Constitution. If this was so, unscrupulous persons would be able to exploit this provision [s 32 of the Constitution] for their own selfish reasons. A balance must be achieved between the right to access to documents and the right to privacy entrenched in section 14 of the Constitution."

52 In relation to public bodies.

53 In relation to private bodies.

54 The AIA contains a list of situations where disclosure would not be unreasonable. See par 4.2.7.3.a below.

55 See further par 4.2.7.3.

appropriate" internal measures providing for such correction until legislation providing for such correction takes effect.[56] The legislation referred to will of course be the data protection legislation envisaged in a previous paragraph.[57]

4.2.4 Scope of AIA

4.2.4.1 Relationship with other legislation

a Legislation restricting access

The AIA does not explicitly or implicitly repeal any other legislation. It does provide, however, that the Act excludes any provision of any other legislation that prohibits or restricts the disclosure of a record of a public or private body if that provision is materially inconsistent with an object or provision of the AIA.[58] This means that legislation that prohibits the disclosure of information outside the context of an AIA request remains valid, but if a request for access falls within the ambit of the AIA, the AIA applies to the exclusion of any other legislation.[59]

b Legislation permitting access

The AIA also provides that nothing in the Act prevents the giving of access to a record of a public or

56 Act 2 of 2000 s 88.

57 See fn 38 and associated text.

58 Act 2 of 2000 s 5.

59 Currie & Klaaren *AIA commentary* 31–32 (par 3.1) give the following example: the Protection of Information Act 84 of 1982, which prohibits disclosure of a wide range of security-related information, no longer applies to a request for a record made in terms of the AIA. A request for access must be considered solely with reference to the provisions of the AIA. However, the Protection of Information Act 84 of 1982 continues to apply to disclosures of information outside the ambit of the AIA. It will eg remain an offence in terms of the former Act to disclose protected information on one's own initiative or informally.

private body in terms of other legislation specifically referred to in a schedule to the AIA.[60] The aim of this provision is to maximise disclosure of records and it "represents a determination by Parliament that certain legislation promotes the constitutional right of access to information".[61]

4.2.4.2 Public and private sector

The AIA applies to both the public and the private sectors in that it grants requesters a right of access[62] to records kept by public and private bodies.[63] In the case of private bodies, access need only be given if the records are required for the exercise or protection of any rights.[64] In regard to public bodies, the

60 Act 2 of 2000 s 6. The only Act listed in the schedule at this point in time is the National Environmental Management Act 107 of 1998. According to Klaaren, Currie & Smith "Access to information legislation" 31 "a significant feature of access to information regimes is their relationship with environmental regulation. Often, access to information legal questions first emerged in this field. The South African regime is an example of this. The primary piece of environmental legislation – the National Environmental Management Act 107 of 1998 – is the only piece of legislation specifically permitted by the AIA to regulate a supplementary but separate access to information scheme". Also see Glazeswki 1999 *Acta Jurida* 1, 14 on the relationship between the access to information clause and "environmental justice". See further Du Plessis 1999 *Obiter* 92.

61 Currie & Klaaren *AIA commentary* 33 (par 3.4). An important issue not dealt with by the AIA is the informal release of information outside the procedures of the Act or any other legislation. Currie & Klaaren *AIA commentary* 36 (par 3.9) argue convincingly that the AIA should not be read as preventing the informal provision of information outside the mechanisms of the Act: "It would be distinctly counter-purposive to read the Act as making access to information more difficult than it was before its enactment." However, as far as data protection is concerned, common law would then be applicable. See ch 7.

62 Act 2 of 2000 s 3.

63 A public body means (a) any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or (b) any other functionary or institution when (i) exercising a power or performing a duty in terms of the Constitution or a provincial Constitution; or (ii) exercising a public power or performing a public function in terms of any legislation. A private body means a natural person or partnership that carries on a trade, business or profession, or a juristic person that is not a public body (see Act 2 of 2000 s 1). A specific body may in certain instances function as a public body, and in others as a private body (see Act 2 of 2000 s 8).

64 Act 2 of 2000 s 50(1)(a). The right to privacy of a personal requester will naturally be included among the rights envisaged by the section. (A question about which there still is uncertainty at this early stage is whether the mere possession of personal information will implicate the privacy right and entitle an individual to access (Pimstone 1999 *SAJHR* 2, 18)). In other cases, the rights probably concern the maintenance of legitimate interests as a ground justifying access to information (see ch 7 par 2.3.2.3.c).

powers and duties conferred by the AIA are entrusted to the information officer[65] of the body in question, while in the case of private bodies the head[66] of the body is the person responsible for giving effect to the Act.

Freedom of information legislation in general does not apply to the private sector, but access to private-sector information is justified in the AIA for the purpose of protecting rights and promoting a human rights culture and social justice.[67] Another innovation of the AIA is that it permits the state to exercise the right of access in regard to information in private hands.[68]

However, it should be noted that certain categories of records, three of which relate to records kept by public bodies or officials of public bodies, are entirely exempt from the provisions of the Act and cannot be the subject of a request in terms of the AIA. They are:

- records requested for criminal or civil proceedings after commencement of the proceedings, where any other law provides for the production of such records[69]

65 The Act contains a very technical definition of an information officer stating that the information officer of a department is the officer designated to a certain position in terms of the Public Services Act of 1994, or otherwise the Director-General, head, executive director or equivalent officer, of that department.

66 The head of a private body, who may be a natural person, partnership or juristic person, is the person duly authorised by the body (see Act 2 of 2000 s 1).

67 Act 2 of 2000 s 9(c); Currie & Klaaren *AIA commentary* 21 (par 2.8).

68 See par below 4.2.4.3. According to Currie & Klaaren *AIA commentary* 19 (par 2.6) the implications are considerable:

> In effect, the Act starts from an assumption that any information in private hands with a demonstrable and sufficient connection to the exercise or protection of any rights legitimately belongs in the public domain. It does this by providing a right to request such information and placing a burden on a private entity to justify why the requested information should not be disclosed. It also allows public bodies to exercise the right, effectively granting a wide and general power to the state to seek information from the private sector to protect its rights or the public interest.

69 Act 2 of 2000 s 7(1).The purpose of this section is to prevent the AIA from having any impact on the law relating to discovery or compulsion of evidence in civil and criminal proceedings (Currie & Klaaren *AIA commentary* 53 (par 4.15)). Also see *CCII Systems (Proprietary) Ltd v Fakie NO* 2002 JDR 0897 (T).

- ❒ a record of the cabinet and its committees[70]
- ❒ records relating to the judicial functions of a court or special tribunal or officer of such court or tribunal[71]
- ❒ records of individual members of Parliament or of a provincial legislature in that capacity[72]

4.2.4.3 Requesters: natural and juristic persons?

A requester is defined both in relation to a public body and in relation to a private body as a person who makes a request for access to a record kept by that body. In relation to a private body the requester may also be a public (government) body, but in relation to a public body certain public bodies are excluded.[73] Requesters are therefore persons, natural or juristic,[74] who request information from private enterprises or government bodies and may even include government bodies themselves.[75] No residence, citizenship or jurisdictional qualifications are required before someone can be a requester.[76]

---

70 Act 2 of 2000 s 12(a). According to Currie & Klaaren *AIA commentary* 54 (par 4.16) fn 37, similar exemptions in Commonwealth jurisdictions are usually justified as aimed at ensuring the long-standing tradition of Cabinet secrecy and the convention of collective ministerial responsibility. These authors also indicate (56–57 (par 4.17)) that although cabinet records are left unregulated by the AIA, they are still subject to the constitutional right of access (unmediated by the AIA).

71 Act 2 of 2000 s 12(b). The purpose of this exemption is "to ensure that the body of rules and procedures that has been developed to ensure the efficient functioning of the courts, the fairness of litigation and the finality of judicial decisions is (sic) not affected by the access to information procedures of the AIA" (Currie & Klaaren *AIA commentary* 57 (par 4.18)).

72 Act 2 of 2000 s 12(c). The purpose of the exemption is "probably to protect freedom of speech and political activity in the legislature and to avoid conflict between the AIA and the internal rules of the legislature pertaining to publication and availability of their records" (Currie & Klaaren *AIA commentary* 58 (par 4.19)).

73 Act 2 of 2000 s 1. State departments and organs of state exercising constitutional powers (eg the courts and the legislature) may not use the AIA to collect information from public bodies. Functionaries and entities exercising public powers or performing a public function in terms of legislation do qualify as requesters (Currie & Klaaren *AIA commentary* 60 (par 5.2)).

74 On the protection of juristic persons as data subjects, see ch 7 par 2.5.2.

75 See the definitions of private and public bodies in fn 63. For a detailed discussion of principles regarding the requester of access to a record, see Visser 2002 *THRHR* 254–259.

76 Currie & Klaaren *AIA commentary* 60 (par 5.2).

However, there is another group of requesters, namely "**personal requesters**". They are requesters seeking access to records containing "personal information" about themselves (ie data subjects).[77] Only natural persons can be personal requesters, since personal information is defined as information about an identifiable individual.[78] This is a shortcoming in the Act, since both common law and constitutional law in South Africa recognise that juristic persona have a right to privacy.[79]

4.2.4.4 Manual and electronic records

The application provisions of the AIA make it clear that the Act applies to "records".[80] The concept controlling the scope of application of the Act is therefore a "record" and not "information".[81] From the definition of "record" as any recorded information regardless of form and medium,[82] it is evident that both manual and computer records are included in the scope of the AIA.

The definition of record is built around the concept of recorded information. Any information recorded in any form by employees of a public or private body in the course of their duties would be included. This includes electronic mail messages, audio or video tapes, computer files, rough notes, notes on notepads and documents in any form.[83] However, the AIA cannot be used to require public or private bodies to compile information or put information in a record.[84] As Currie and Klaaren[85] put it, "the Act

77 Act 2 of 2000 s 1. Note that according to s 1 personal information does not include information about individuals who have been dead for more than 20 years. On the issue of whether deceased persons should be considered to be "individuals" worthy of protection in data privacy protection legislation, see ch 7 par 2.5.1. Also see Wessels 2002 (Mar) *De Rebus* 28 on the possibility of a student requesting access to his or her marked examination paper as a "personal requester".

78 Act 2 of 2000 s 1. See fn 200 for the complete definition.

79 See ch 7 par 2.5.2.

80 Act 2 of 2000 s 3–8.

81 Currie & Klaaren *AIA commentary* 41 (par 4.1).

82 Act 2 of 2000 s 1.

83 Currie & Klaaren *AIA commentary* 41 (par 4.1).

84 The AIA does not require public or private bodies to create or retain records (Currie & Klaaren *AIA* (continued...)

does not oblige public or private bodies to act as researchers but only as a research source". This does not mean that electronic data in a database should be excluded from the concept of "record", because technically such data are not "recorded information" but raw data that must still be processed to produce a record. After all, the production of a record based on data in a database is a routine function of databases and retrieval software.[86]

The AIA applies to all records, regardless of when they came into existence.[87] In order to qualify as "a record of the body" the record must be under the control of the body to whom the request is made.[88] The body need not necessarily have created the record.[89]

4.2.5 Index of records

Before individuals can request access to personal information, they have to have knowledge of the fact that personal information about them may possibly be held by a specific body.[90] The AIA consequently provides that the information officer of a public body or the head of a private body should publish a manual[91] containing *inter alia*:

84(...continued)
commentary 45 (par 4.6)). Also see Visser 2002 *THRHR* 254, 255.

85 Currie & Klaaren *AIA commentary* 42 (par 4.1).

86 Currie & Klaaren *AIA commentary* 42 (par 4.2).

87 Act 2 of 2000 s 3.

88 From comparative research, the following factors have been identified as relevant in determining whether an institution controls a record: the intent of the record's creator to retain or relinquish control over the record; the ability of the institution to use and dispose of the record as it sees fit; the extent to which the institution or its personnel have read or relied upon the record; and the degree to which the record was integrated into the institution's record keeping system or files (see Currie & Klaaren *AIA commentary* 44 (par 4.4)).

89 Currie & Klaaren *AIA commentary* 43 (par 4.4).

90 See also the discussion of the openness principle of data protection above (ch 6 par 2.2.7).

91 Act 2 of 2000 s 14 and s 51.

- the postal and street address, telephone and fax number and electronic mail address of the information officer (and of every deputy information officer)[92] or the head of the private body[93]

- a description of the guide compiled by the Human Rights Commission on how to use the Act,[94] and how to obtain access to the guide

- a description of the categories of records of the public or private body which are available without a person having to request access in terms of the Act[95]

- a description of the records of the body which are available in terms of other legislation

- sufficient detail to facilitate a request for access to a record held by the body, a description of the subjects on which the body holds records and the categories of records held on each subject

The Minister may exempt bodies from the above provisions for security, administrative or financial reasons.[96] Apart from this manual, there are no mandatory provisions in the AIA requiring own-initiative

92 The Act makes provision for the designation of deputy information officers in order to render public bodies as accessible as reasonably possible for requesters of records (Act 2 of 2000 s 17(1)).

93 The Director-General of the national department responsible for government communication and information services must ensure that the contact information of the information officers of all public bodies is published in every telephone directory issued for general use by the public (Act 2 of 2000 s 16). There is no similar provision for private bodies in the Act.

94 See Act 2 of 2000 s 10. The guide must *inter alia* include a description of the objects of the Act, contact information about the information officers of all public bodies, such particulars of private bodies as may practicably be furnished, the manner and form of a request to access a record held by either a public body or a private body, the assistance available from the information officers of a public body as well as from the Human Rights Commission and all remedies in law available in terms of the Act.

95 The information officer of a public body must, and the head of a private body may, submit to the relevant Minister a description of the categories of records that are automatically available. The Minister must then publish such information in the *Government Gazette* (see Act 2 of 2000 s 15 and 52).

96 See Act 2 of 2000 s 15(5) and 15(4).

disclosure of records.[97]

4.2.6 Request for access

4.2.6.1 Introduction

The AIA gives effect to the Constitutional demand for access to information by giving persons the right to request information in a record and by imposing a duty on private and public bodies to provide the information requested, unless there is a ground for refusing the request, in which case the body refusing the access has the burden of justifying the refusal.[98] It is always the head of a private body or the information officer of a public body who has the authority to grant or deny access. The AIA confers responsibility on the most senior official in a government body or private organisation for ensuring that the responsibilities imposed by the Act are taken seriously.[99] The Act permits written delegation of the powers and duties of the information officer to deputy information officers.[100]

As far as public bodies are concerned, a requester's right of access is not affected by the reasons why access is requested, but "manifestly frivolous or vexatious requests" may be refused.[101] Access to records kept by private bodies need only be given if the record is required for the exercise or protection of any rights.[102]

---

97 Currie & Klaaren *AIA commentary* 59 (par 5.1) fn 1.

98 It is compulsory to give access to records to a person requesting access where that person has complied with the procedural requirements of the Act (see Act 2 of 2000 s 11(1) and s 50(1)).

99 See Currie & Klaaren *AIA commentary* 73 (par 6.1) fn 1.

100 Act 2 of 2000 s 17(3). Implied delegation is not possible, since the delegation must be in writing.

101 Act 2 of 2000 s 11(3). Notwithstanding the provision that the reason for the request is not relevant, in one situation the reason for the request would be relevant: a request for access has to be refused where the reason for the request is to obtain a document for purposes of litigation, if the record is governed by the law pertaining to discovery (this is so because of s 7 which exempts from the Act records requested for purposes of litigation). See par 4.2.4.2; also see Currie & Klaaren *AIA commentary* 64 (par 5.6).

102 Act 2 of 2000 s 50(1)(a). In *Cape Metropolitan Council v Metro Inspection Services CC* 2001 3 SA 1013 (SCA) 1026 the right of access to information under s 32 of the Constitution was at issue. Streicher JA held

(continued...)

4.2.6.2 Fees

A right of access to records under the AIA and the duty to consider requests only arise once the requester has complied with the procedural requirements of the Act. These include the paying of a prescribed fee.[103] The fee provision of the Act can be seen as "a reasonable measure to alleviate the administrative and financial burden on the state" as permitted by section 32(2) of the Constitution of 1996.[104] The Minister may, by notice in the *Gazette*, regulate the fees to be paid.[105]

The Act provides for two kinds of fees to be paid by a requester: a request fee and an access fee, including a deposit in respect of the access fee.[106] The request fee is payable when the request for access is made. The access fee is paid when access is given to the record, and includes the cost of reproduction of the record, postal fees if any, and the time spent on searching for and preparing the record for access.[107]

From a data protection point of view, it is important to note that personal requesters, in other words persons requesting information relating to themselves, are expressly excluded from the section requiring

---

102(...continued)
that information can only be required for the exercise or protection of a right if it will be of assistance in the exercise or protection of the right. In order to make out a case for access to information an applicant therefore has to state what the right is that he or she wishes to exercise or protect, what information is required and how that information would assist him or her in exercising or protecting that right. In *Andrew Christopher Davis v Clutcho (Pty) Ltd* (unreported decision of the Cape of Good Hope Provincial Division of 10 June 2003, case no 1289/03) the court held that the word "required" in s 50 must be understood to mean "reasonably required" as opposed to simply "needs" or "desires".

103 Currie & Klaaren *AIA commentary* 71 (par 5.13).

104 Currie & Klaaren *AIA commentary* 71 (par 5.13).

105 Act 2 of 2000 s 22(8) and 54(8). The Minister may eg exempt any person or category of persons from paying any fees, determine that a fee may not exceed a certain amount, determine the manner in which a fee must be calculated, or determine that no fee need be paid on certain categories of records.

106 Act 2 of 2000 s 22 and s 54.

107 Act 2 of 2000 s 22(7) and 54(7).

that a request fee should be paid.[108] They are also not required to pay a deposit before the request is processed, but they have to pay an access fee.[109]

4.2.6.3 Form of request

A request for access must be made in the prescribed form at the relevant address, fax number or electronic mail address.[110] From this one can deduce that the request must be in writing. However, in the case of a request for access to a record held by a public body, a request may be made orally if the requester is unable to make the request in writing owing to illiteracy or a disability.[111] The information officer must then reduce the request to writing and provide a copy to the requester.[112]

The prescribed form must require at least the following from the requester:[113]

- to provide sufficient particulars to enable identification of the requester and the records requested
- to indicate the form of access required[114]
- in the case of public bodies, to state whether the record is required in a particular language[115]
- to specify a postal address or fax number for the requester in the Republic
- in the case of private bodies, to identify the right the requester is seeking to exercise or protect and provide an explanation of why the requested record is required for the exercise of that

108 Act 2 of 2000 s 22(1) and s 54(1).

109 See Act 2 of 2000 s 22(6) and s 54(6).

110 Act 2 of 2000 s 18(1) and 53(1).

111 Act 2 of 2000 s 18(3)(a).

112 Act 2 of 2000 s 18(3)(b).

113 Act 2 of 2000 s 18(2) and 53(2).

114 On the forms of access, see par 4.2.6.10.

115 See further par 4.2.6.10.

right[116]

- ❒ if, in addition to a written reply, the requester wishes to be informed of the decision on the request in any other manner, to state that manner and the necessary particulars to make it possible for the requester to be so informed
- ❒ if the request is made on behalf of a person, to submit proof of the capacity in which the requester is making the request, to the reasonable satisfaction of the information officer of the public body or head of the private body

It is submitted that a request should not be refused for lack of compliance with all the requirements of the prescribed form, as long as there is substantial compliance with it.[117] This interpretation is in line with the duty to assist requesters, which will be discussed next.

4.2.6.4 Duty to assist (public body)

The AIA[118] imposes extensive duties on information officers of public bodies to assist requesters, before a request may be refused on the grounds of noncompliance with the requirements of the prescribed form. This duty has both a "pro-active and re-active" element.[119] The pro-active part provides that if a requester informs the information officer of a public body that he or she wishes to make a request for access to records of that public body, or the records of another public body, the information officer

116 As stated, a right of access to the records of private bodies only exists if those records are required for the exercise or protection of any rights (Act 2 of 2000 s 50(1)(a)). Since it is for the protection of "any" rights, the right need not necessarily be that of the requester (Currie & Klaaren *AIA commentary* 65 (par 5.7)); Ferreira 2000 *SAPR/PL* 527, 538. This provision is important for data protection, because it embodies the idea that access to personal records is permitted for the maintenance of a legitimate private or public interest (see ch 7 par 2.3.2.3.c). For this reason, the interpretation by Currie & Klaaren *AIA commentary* 70–71 (par 5.12) of rights to mean "fundamental rights"where the request for access is to records in private hands seems to be too restrictive. Also see *Cape Metropolitan Council v Metro Inspection Services CC* 2001 3 SA 1013 (SCA) 1026 where Streicher JA held that under s 32 of the Constitution "rights" included all rights and not only fundamental rights.

117 According to Currie & Klaaren *AIA commentary* 62 (par 5.4) "(t)he principal purpose of the Act – the promotion of access to information – is not served by placing formalistic barriers in the way of information requesters".

118 Act 2 of 2000 s 19.

119 See Currie & Klaaren *AIA commentary* 63 (par 5.5).

must render, free of charge, reasonable assistance to enable the requester to make the request in the prescribed form.[120]

The reactive part provides that on receipt of a request that does not comply with the prescribed form, the request should not be refused as long as there is substantial compliance.[121] Also, a public body may not refuse a request for access that does not (substantially) comply with the prescribed form for access, unless the public body has notified the requester that the request does not comply with the prescribed form, has offered assistance to put the request in the correct form, has given the requester a reasonable opportunity to seek such assistance, has supplied the information necessary to make the changes, and has given the requester a reasonable opportunity to confirm or amend the request.[122]

If a request for access to a record has been made to the wrong public body, the information officer must either transfer the request to the relevant public body, or assist the requester to make the request to the relevant body, whichever will result in the request being dealt with earlier.[123]

Private bodies are not burdened with the duty to assist requesters, but requesters may be assisted by the Human Rights Commission.[124]

4.2.6.5 Transfer of request (public body)

Where a request for access to a record is made to a public body, but the record is in the possession or under the control of another public body, the body may not refuse the request on this basis. Instead, it is required to re-direct the request to the other body. The public body may also re-direct the request

120 Act 2 of 2000 s 19(1).

121 See par 4.2.6.10.

122 Act 2 of 2000 s 19(2). The period used to rectify the request will be disregarded when calculating the time that the public body has to respond to a request (Act 2 of 2000 s 19(3)).

123 Act 2 of 2000 s 19(4).

124 Act 2 of 2000 s 83(3)(c). Also see Currie & Klaaren *AIA commentary* 74 (par 6.2).

to another body if the record's subject matter is more closely related to the functions of the other public body, or the record contains commercial information in which another public body has a greater commercial interest. This has to be done as soon as is reasonably possible, but in any event within fourteen days after receiving the request. A copy of the record should also be sent with the request, if the record is in the possession of the body to which the request was made, and it will be helpful to do so.[125]

The aim of this provision is to ensure that officials who are familiar with the subject matter of a record deal with a request for access to that record.[126]

Where a request for access to a record is made and the information officer does not know who has control of the record, or which public body's functions are more closely related to the record, the request can be transferred to the public body for which the record was first created or which first received the record.[127]

In order to prevent the response to a request for access from being delayed as a result of the transfer of the record, the Act provides that the information officer to whom the request is relayed should give priority to it as if he or she had received it on the day the information officer who relayed the request received it.[128] The requester must immediately be informed about the transfer, the reasons for it, and the time within which the request must be dealt with.[129]

Public bodies do not have a duty to transfer requests to private bodies, and neither have private bodies

125 Act 2 of 2000 s 20(1).

126 Currie & Klaaren *AIA commentary* 80 (par 6.7).

127 Act 2 of 2000 s 20(2).

128 Act 2 of 2000 s 20(3). However, when calculating the time within which the public body is obliged to respond to a request, the date on which the officer to whom the request was transferred received the request is the relevant date (Act 2 of 2000 s 20(4)).

129 Act 2 of 2000 s 20(5).

a duty to transfer a misdirected request.[130]

4.2.6.6 Third party notification and intervention

The grounds for refusal of a request to access distinguish between two general classes of records: records that contain information that relates to a third party,[131] or records that contain information belonging to the public or private body that is the recipient of the request.

Where a request for access to a record is being considered by a private or public body and the record might be one where there is a mandatory ground for refusal present because the record contains information[132] relating to a third party,[133] the body must take all reasonable steps necessary to inform the third party of the request.[134] The third party should be informed by the fastest practicable means and as soon as is reasonably possible (but in any event within twenty-one days of receipt of the request for access).[135] The third party must be informed about[136]

130 Currie & Klaaren *AIA commentary* 81 (par 6.7).

131 Ie, a party that is not involved in the request, either as a requester or as a recipient.

132 Personal, tax, commercial, confidential, or research information relating to the third party.

133 The third party grounds for refusal require mandatory refusal of access (see Act 2 of 2000 s 63–67 and see further par 4.2.7).

134 Act 2 of 2000 s 47(1) and 71(1). This reflects the active control principle that an individual must have the right to require from the data controller information as to the identity of all persons who have had access to his or her data. This will enable him or her to ascertain whether or not the information was used for the protection of a legally recognised interest. See ch 7 par 4.2.4. It is also a reflection of the openness principle of data protection (see ch 6 par 2.2.7).

135 Act 2 of 2000 s 47(2) and 71(2).

136 Act 2 of 2000 s 47(3) and 71(3). The Act requires written notice to be given about this information. In the case of a public body, the Act states that the written notice must be given if "a third party is *not* informed orally of a request for access" (s 47(4) – my emphasis), whereas in the case of a private body the written notice must be given "if a third party is informed orally of a request for access" (s 71(4)). The Afrikaans version of the Act contains the term *nie* in both instances. It would therefore seem that a written notice need only be given if the third party is initially informed in writing about the request. If the third party is orally informed about the request for access the notice need not be given in writing, but presumably all the other information must nevertheless be given, albeit orally.

- ❒ the fact that a record is involved that contains information relating to him or her
- ❒ the content of the record
- ❒ the name of the requester
- ❒ the grounds for refusal that may be present
- ❒ the fact that a mandatory ground for access may be present,[137] including the reasons why the body thinks such a ground may be present
- ❒ the fact that the third party may make written or oral representations that the request for access should be refused, or may give written consent for the disclosure of the record, within twenty-one days

Where the third party obtains knowledge about a request for access in another manner, the third party may also make written or oral representations that the request for access be refused, or give written consent for the disclosure of the record.[138]

The head of the body must, as soon as reasonably possible but in any event within thirty days after all third parties have been informed, and after considering all the representations received, decide whether to grant the request for access.[139] Where third parties have not been informed, despite all reasonable steps taken, any decision whether to grant the request or not should be made with due regard for this fact.[140] The third parties involved should be informed about:[141]

- ❒ the decision reached
- ❒ the reasons for the decision, which must be adequate, and the provisions of the Act relied upon
- ❒ the third party's right to lodge an internal appeal (in the case of a public body) or an application

137 In terms of Act 2 of 2000 s 46 and 70 the public interest in disclosure may outweigh the individual's right to keep the information confidential (see text to fn 181).

138 Act 2 of 2000 s 48(2) and 72(2).

139 Act 2 of 2000 s 49(1) and 73(1).

140 Act 2 of 2000 s 49(2) and 73(2).

141 Act 2 of 2000 s 49(3) and 732(3).

to court against the decision within thirty days

- the fact that the requester will be given access to the record within thirty days unless an appeal or court application has been lodged

4.2.6.7 Records that cannot be traced

If, after taking all reasonable steps to find a requested record, it is believed on reasonable grounds that the record cannot be traced or does not exist, the information officer or head of a private body must notify the requester that access cannot be given.[142] Such notice is regarded as a refusal of a request for access.[143] This notice must take the form of an affidavit or affirmation and must give a full account of all the steps taken to find the record or determine whether it exists or not, including all communications with every person who conducted the search on behalf of the information officer or head of the private body.[144] Should the record be found afterwards, the requester must be given access thereto, unless access is refused on one of the grounds for refusal listed in the Act.[145]

4.2.6.8 Preservation of records until final decision on request (public body)

If a public body has received a request for access to a record, such record may not be destroyed or information deleted from it, until a decision has been made on the request to access and the requester has been informed about it, and further remedies provided by the Act have been employed or the time for such remedies has elapsed.[146]

4.2.6.9 Decision on request and notice thereof

142 Act 2 of 2000 s 23(1) and s 55(1).

143 Act 2 of 2000 s 23(3) and s 55(3).

144 Act 2 of 2000 s 23(2) and s 55(2).

145 Act 2 of 2000 s 23(4) and s 55(4).

146 Act 2 of 2000 s 21. In my opinion this provision should have been extended to private bodies as well.

a Introduction

The information officer of a public body, or the head of the private body, to whom a request for access has been made, may grant or refuse or defer a request for access. The Act does not grant the power to impose conditions on the subsequent use of records that have been disclosed.[147]

The recipient of the request for access has thirty days in which to decide whether to grant a request for access or not,[148] and to notify the requester of his or her decision.[149] Failure to give a decision within this period is regarded as a refusal of the request.[150]

If a request for access relates to a record that contains both information to which access may or must be refused and other information that may be disclosed, the latter information should be disclosed if it can reasonably be severed from the other information.[151] The severance provision is in accordance with the principle that limitations of the right to access should be reasonable and proportional to the aims pursued by the limitation. It is therefore not competent for a body to refuse access to a record because it contains some information that is covered by a ground for refusal of access. If that information can be deleted from the record, the rest of the information in the record must be disclosed.[152]

147 Currie & Klaaren *AIA commentary* 97 (par 6.24). However, such use will be subject to the general law. Eg, if the information is defamatory, subsequent publications of the information may lead to an action for defamation.

148 The period may be extended once for a further period of thirty days if the requester consents to such extension, or if the search cannot reasonably be completed within the first period for specified reasons (see Act 2 of 2000 s 26(1) and s 57(1)).

149 Act 2 of 2000 s 25(1) and s 56(1). If the requester has specified a specific manner in which to be notified, that manner must be used if reasonably possible.

150 Act 2 of 2000 s 27 and s 58. The Act provides for extended periods to deal with requests during the first two years after the Act has taken effect (Act 2 of 2000 s 87).

151 Act 2 of 2000 s 28 and s 59.

152 See also Currie & Klaaren *AIA commentary* 90 (par 6.15).

b Request granted

If the request is granted, the notice must state the access fee to be paid and the form in which access will be granted. The requester must also be informed of the remedies available in terms of the Act,[153] if he or she is not satisfied with the fee to be paid or the manner in which access will be given.[154]

c Request refused

If the request for access is refused, the notice must state adequate reasons for refusal, including the provision of the Act to which recourse was had. The reasons may not refer to the content of the record. The requester must also be informed of the remedies available in terms of the Act against the refusal.[155] Reasons for the refusal will be adequate if they enable the requester to make an informed decision whether to use his or her remedy of appeal.[156]

As stated previously, failure to give a decision within the prescribed period is deemed to be a refusal of the request.[157] The deemed refusal provision is designed to prevent a requester from being frustrated by an unresponsive public body and it allows a requester to make use of the dispute-resolution mechanisms of the Act.[158]

d Deferral of access (public body)

If the information officer of a public body decides to grant a request for access to a record, but that

153 Internal appeal (in the case of a public body) and application to a court.

154 Act 2 of 2000 s 25(2) and s 56(2).

155 Act 2 of 2000 s 25(3) and s 56(3).

156 Currie & Klaaren *AIA commentary* 93–94 (par 6.20).

157 Act 2 of 2000 s 27 and s 58. The Act provides for extended periods to deal with requests during the first two years after the Act has taken effect (Act 2 of 2000 s 87).

158 Currie & Klaaren *AIA commentary* 95 (par 6.22).

record is to be published or submitted to a legislature or other person in any event, the request for access may be deferred for a reasonable period.[159] It should be emphasised that deferral is a discretionary decision to defer the date on which access to a record is granted – it is the date of access that is deferred, not the decision to grant access or refuse it.[160]

The purpose of this provision is to protect documents, that are shortly to be published or otherwise made publicly available, from harm that may result from premature disclosure. The request for access may only be deferred for a "reasonable" period. The reasonableness or otherwise of the period should be determined with reference to the purpose of the provision.[161]

The requester must be informed of the likely period for which the access will be deferred, and of his or her right to make representations for earlier access.[162] If such a request is made, it may only be granted if there are reasonable grounds for believing that the requester will suffer "substantial prejudice" if access is deferred.[163] In order to enable the recipient of the request to decide whether substantial prejudice will ensue, the requester will have to provide reasons why the information is required urgently. These reasons are not relevant in deciding whether to grant access or not, but are relevant in deciding whether access should be deferred or not.[164]

4.2.6.10 Forms and language of access

a Private bodies

159 Act 2 of 2000 s 24(1).

160 Currie & Klaaren *AIA commentary* 85 (par 6.11).

161 Currie & Klaaren *AIA commentary* 85 (par 6.11).

162 Act 2 of 2000 s 24(2).

163 Act 2 of 2000 s 24(3).

164 Currie & Klaaren *AIA commentary* 85 (par 6.11). Also see fn 101.

In the case of a private body, if access is granted to a record held by that body, the access must be given as soon as reasonably possible in the form requested by the requester, or if no specific form is required, in such form as may reasonably be determined by the head of the body.[165] No requirements are laid down as to the language in which access has to be given.

b Public bodies

The Act contains more detailed provisions that apply when access is granted to the records of public bodies. Access should be given immediately after the requester has been informed that his or her request for access has been granted, unless a fee is payable, in which case access should be given upon payment of that fee.[166] Where an internal appeal has been lodged, or an application has been made to a court against the granting of a request for access, access may only be given when the decision to grant the request is finally confirmed.[167]

Access should be given in the language requested. If the record does not exist in the language preferred, or no preference has been stated, access is given in the language in which the record exists.[168]

Access should also be given in the form requested, unless to do so would interfere unreasonably with the effective administration of the public body, or would be detrimental to the preservation of the record, or would amount to an infringement of copyright not owned by the State.[169] If access is given in some other form than the form requested, the fee payable may not exceed that which the requester would have paid for the requested form.[170] If the requester is unable to read, view or hear the record

165 Act 2 of 2000 s 60.

166 Act 2 of 2000 s 29(1).

167 Act 2 of 2000 s 29(9).

168 Act 2 of 2000 s 31.

169 Act 2 of 2000 s 29(3).

170 Act 2 of 2000 s 29(4).

in the form held by the public body because of a disability, the information officer must take reasonable steps to make the record available in a form in which the requester is capable of reading, viewing or hearing the record.[171] The fee payable by the disabled requester may not be increased because of his or her special requirements.[172]

If no form is requested, the forms in which access will be given are the following:[173]

- ❒ if the record is in written or printed form, by supplying a copy of the record or by making arrangements for the inspection of the record
- ❒ if the record consists of visual images, by reproducing the visual images or making a printed transcription by means of equipment ordinarily available to the public body
- ❒ if the record consists of sound recordings, by arranging for the sound recording to be heard, or by transcribing it on equipment ordinarily available to the public body
- ❒ if the record is held on the computer or in electronic or machine-readable format, by producing a printed copy of the record or the information derived from the format in which the record is held

If a record is made available for inspection, viewing or listening to, the requester may transcribe the record using his or her own equipment, unless to do so would interfere unreasonably with the effective administration of the public body, or would be detrimental to the preservation of the record, or would amount to an infringement of copyright not owned by the State.[174] Where the Act requires that a copy of the record should be given, the copy should be posted to the requester.[175]

171 Act 2 of 2000 s 29(6).

172 Act 2 of 2000 s 29(6).

173 Act 2 of 2000 s 29(2).

174 Act 2 of 2000 s 29(7).

175 Act 2 of 2000 s 29(8).

4.2.6.11 Access to health records

Where an information officer or the head of a private body grants access to any health records but is of the opinion that the disclosure of the record would cause serious physical or mental harm to the person to whom the information relates (the relevant person), the officer or head may first consult with a health practitioner.[176] If the health practitioner, who is to be nominated by the relevant person or someone acting on his or her behalf, agrees with the view of the officer or head, access may only be given to the record after arrangements have been made by the relevant person for counselling, and such arrangements have proved satisfactory to the head or information officer.[177] The person providing the counselling must be given access to the records before the relevant person is given access.[178] In essence this section permits sensitive medical or psychiatric information to be released indirectly through a medical practitioner.[179]

This provision is important from a data protection perspective, because it places a limitation on an individual's right to access his or her medical records in specific circumstances. However, since the aim is to protect the health of the data subject, it is a valid limitation.

4.2.6.12 Summary of procedure for dealing with requests[180]

After receiving a request for access to a record which substantially complies with the formal requirements of the Act and on receipt of the prescribed application fee, the information officer or the head of a private body must consider the following:

176 Act 2 of 2000 s 30(1) and 61(1).

177 Act 2 of 2000 s 30(3)(a) and 61(3)(a).

178 Act 2 of 2000 s 61(3)(b) and 61(3)(b).

179 Currie & Klaaren *AIA commentary* 89 (par 6.14).

180 This summary is from Currie & Klaaren *AIA commentary* 74–75 (par 6.3).

Requests to public bodies

- ❒ whether the request should be transferred to another public body
- ❒ whether third parties should be notified
- ❒ whether the request should be granted or refused (including whether the record may be reasonably severed)
- ❒ If the request is to be granted:
  - – whether access to the record is to be deferred for a reasonable period
  - – in which form access is to be given
  - – whether an access fee is payable
- ❒ If the request is to be refused:
  - – the requester must be informed and given adequate reasons for the refusal

Requests to private bodies

- ❒ whether third parties should be notified
- ❒ whether the request is to be granted or refused (including whether the record may be reasonably severed)
- ❒ If the request is to be granted:
  - – in which form access is to be given
  - – whether an access fee is payable
- ❒ If the request is to be refused:
  - – the requester must be informed and given adequate reasons for the refusal

4.2.7 Grounds for refusal of access

4.2.7.1 Public interest override

Once a request for access has been received in the prescribed form and with payment of the prescribed

fees, the AIA requires that access be granted unless a ground for refusal of access is mandated or permitted. However, if the disclosure of the record would reveal evidence of a substantial contravention of, or failure to comply with, the law, or an imminent and serious public safety or environmental risk, and the public interest in having the record disclosed outweighs the harm contemplated by a ground for refusal, the record must be disclosed.[181] In other words, if a ground for refusal of access is not present, access must be granted. If a ground for refusal is present, access can be denied unless the public interest override is applicable, in which case access must also be granted.

The public interest that is protected by this provision is defined by the provision as the law, public safety and the environment. The disclosure of the record must reveal evidence that these aspects of the public interest are at risk. However, this is not enough – the next part of the provision provides that the public interest in disclosure should outweigh the harm contemplated by a refusal of disclosure. A two-pronged test should therefore be applied.

4.2.7.2 Overview of grounds for refusal

Each of the grounds for refusal of access aims to protect a certain identifiable interest or right, such as the right to privacy or property, commercial interests, public safety, administration of justice, defence and international obligations. Some of the grounds are mandatory (ie access must be refused) and others are discretionary (access may be refused). As a general rule, it can be stated that where the rights or interests of third parties are involved, refusal is mandatory. Where the rights or interests of the body that holds the record are implicated, refusal is in the discretion of the body.[182]

The AIA provides that if the records to which access is requested involve one of the following rights or interests, there is a mandatory ground for refusal of access:

181 Act 2 of 2000 s 46 and 70. S 46 provides for mandatory disclosure in the public interest in the case of public bodies in relation to all records except certain records of the SARS (see s 35). S 70 provides for the mandatory disclosure in the public interest in the case of private bodies in respect of all records. See further Currie & Klaaren *AIA commentary* 107– 110 (par 7.10–7.13).

182 Currie & Klaaren *AIA commentary* 106 (par 7.7).

- ❒ the privacy of a third party who is a natural person[183]
- ❒ commercial information on a third party[184]
- ❒ confidential information relating to a third party[185]
- ❒ research information on a third party [186]
- ❒ the safety of individuals[187]
- ❒ certain records of SARS[188]
- ❒ police dockets in bail proceedings and the protection of law enforcement[189]
- ❒ privileged documents[190]

The following discretionary grounds for refusal of access are provided for:

- ❒ defence, security and international relations[191]
- ❒ the economic interests and financial welfare of the RSA[192]
- ❒ commercial information held by public and private bodies[193]
- ❒ research information of a private or public body[194]

183 Act 2 of 2000 s 34 and s 63. See further par 4.2.7.3.

184 Act 2 of 2000 s 36(1) and 64(1).

185 Act 2 of 2000 s 37(1)(a) and s 65. See further par 4.2.7.3.

186 Act 2 of 2000 s 43(1) and s 69(1).

187 Act 2 of 2000 s 38(a) and s 66(a). See further par 4.2.7.3.

188 Act 2 of 2000 s 35(1). See further par 4.2.7.3.

189 Act 2 of 2000 s 39(1). See further par 4.2.7.3.

190 Act 2 of 2000 s 40 and s 67.

191 See Act 2 of 2000 s 41(1)(a).

192 Act 2 of 2000 s 42(1). See further par 4.2.7.3.

193 Act 2 of 2000 s 42(3) and 68(1).

194 Act 2 of 2000 s 43(2) and s 69(2).

- ❒ operations of public bodies[195]
- ❒ safety of property[196]
- ❒ frivolous or vexatious requests[197]

Not all of the grounds for refusal aim to protect privacy and consequently they are not all relevant for data protection purposes. Those grounds that aim to protect the privacy of a data subject, either by refusing a third party access to the record containing information on the data subject, or by permitting the data subject (or a "personal requester" in the terminology of the AIA) access to a record despite the presence of a ground for refusal, will be discussed in more detail.

4.2.7.3 Grounds relevant for data protection

a Privacy of third party who is a natural person

Access to information kept by a private or public body must be refused where the disclosure of the information would involve the unreasonable disclosure of personal information about a third party,[198] including a deceased person.[199] For this ground to be applicable, it must therefore be determined whether the content of the record is personal information (of which the AIA gives a detailed definition),[200] and it must be established that the disclosure of this information would be "unreasonable".

195 Act 2 of 2000 s 44(1). See further par 4.2.7.3 as regards evaluative material held by public bodies.

196 Act 2 of 2000 s 38(b) and s 66(b).

197 Act 2 of 2000 s 45.

198 See fn 131 for the definition of a third party.

199 Act 2 of 2000 s 34 and s 63. However, personal information does not include information about individuals who have been dead for more than 20 years (see Act 2 of 2000 s 1).

200 According to Act 2 of 2000 s 1, "personal information" means information about an identifiable individual, 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 individual;
(b) information relating to the education or the medical, criminal or employment history of the individual
(continued...)

It is submitted that the disclosure of personal information would be unreasonable if it amounted to an unjustifiable violation of the third party's privacy,[201] in other words, if there was no ground of justification, such as the maintenance of a legitimate private or public interest,[202] present to justify the violation.[203]

From the definition of personal information as "information about an identifiable individual", the following general characteristics can be listed:[204]

❒ Personal information is confined to information about human beings.[205]

200(...continued)
or information relating to financial transactions in which the individual has been involved;
(c) an identifying number, symbol or other particular assigned to the individual;
(d) the address, fingerprints or blood type of the individual;
(e) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;
(f) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature or further correspondence that could reveal the contents of the original correspondence;
(g) the beliefs or opinions of another individual about the individual;
(h) the beliefs or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the beliefs or opinions of the other individual; and
(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than 20 years.

201 Also see Currie & Klaaren *AIA commentary* 122 (par 8.8).

202 See also Act 2 of 2002 s 50(1)(a) which provides that access to information in private hands need only be given if it is necessary for the exercise or protection of any rights.

203 See Govender "Limitation on access to information" 22–23 who explains the requirements of the privacy exception as follows:

> This exception requires the information officer to consider two separate requirements, and determine whether the information falls within the zone of non-disclosure created by a combination of these requirements. These requirements must be read with the built-in limitations which expressly state that certain types of information are excluded from this zone. Once the information is deemed to fall within this zone, it must not be divulged. The two separate requirements are:
> - The disclosure must invade the privacy of a third party who is a natural person.
> - Disclosing the information must be unreasonable in the circumstances.

204 See also Currie & Klaaren *AIA commentary* 125 (par 8.13–8.15).

205 Ie, juristic persons are excluded.

- Personal information is "about" an individual, in other words it must convey some information about the individual.[206]
- Personal information is information identifying an individual.[207]

The Act lists several exceptions to the mandatory protection of the privacy of a third party.[208] These exceptions can be considered to be examples of situations where the disclosure of personal information would not be unreasonable, either because the right to privacy is not infringed, or because such infringement is justified.[209]

Access to a record may not be refused where the record consists of information –

- about an individual who has consented in writing to its disclosure to the requester concerned[210] (this would have taken place in terms of the third party notification procedure)[211]
- that is already publicly available[212]
- that was given to the public or private body by the individual to whom it relates and the individual was informed that the information belongs to a class of information that would or

206 Eg, if an individual's name appears in a context that conveys no information about the person, it does not constitute information about the individual (Currie & Klaaren *AIA commentary* 125 (par 8.14)).

207 "No matter how intimate the subject-matter of the record, if it does not identify the person to whom it pertains it is not personal information" (Currie & Klaaren *AIA commentary* 125 (par 8.15)).

208 See Act 2 of 2000 s 34(2) and 63(2).

209 See also Currie & Klaaren *AIA commentary* 122–123 (par 8.9).

210 Consent excludes wrongfulness and thus makes disclosure reasonable. See ch 7 par 2.3.2.3.

211 See par 4.2.6.6.

212 If the information is publicly available, it can no longer be considered private. A *caveat* should be added, however: if the record entails a newly created compilation of individual pieces of information not previously grouped together, creating a profile of the individual, the information is being used in a manner not previously envisaged when the initial separate pieces of information were made available and the privacy of the individual is again at risk. See ch 7 par 2.3.2.2.

might be made available to the public[213]

- about an individual's physical and mental health, or well-being, where the individual is under the care of the requester and is under the age of eighteen years or is incapable of understanding the nature of the request, if giving access would be in the individual's best interests[214]

- about an individual who is deceased, and the requester is the individual's next of kin, or is making the request with the written consent of the next of kin[215]

- about an individual who is or was an official of a private or public body and the information requested relates to the position or functions of the individual[216]

b Confidential information relating to third party

Section 37(1)(a) and section 65 prohibit disclosure of information in circumstances that would entail a breach of confidence owed to a third party in terms of an agreement.[217] Currie and Klaaren interpret this exception as protecting the public interest in the effective regulation of transactions by contract –

213 This amounts to implied consent. Also see Currie & Klaaren *AIA commentary* 127 (par 8.19).

214 This exception is aimed at the best interests of the individual involved who is either a minor or mentally incapable and it involves health information. It can be compared with the "vital interest" ground for the processing of personal data of the EU Directive on data protection (see ch 3 par 4.2.4.2).

215 The definition of personal information includes information of individuals who have been dead for less than twenty years. However, see ch 7 par 2.5.1 where it is argued that deceased persons do not have personality rights and therefore do not have a right to privacy.

216 Such information includes, but is not limited to, the fact that the individual is or was an official of that body, the title, work address, work phone number and other similar particulars on the individual, the classification, salary scale or remuneration and responsibilities of the position held or services performed by the individual, and the name of the individual on a record prepared by the individual in the course of employment (Act 2 of 2000 s 34(2)(f) and 63(2)(f)).

217 Act 2 of 2000 s 37(1)(a) and s 65.

pacta sunt servanda.[218] The public interest override is applicable.[219] This provision is important for data protection since it may protect the privacy of a third party. (Therefore it and the previous ground may overlap).

c Safety of individuals

Section 38(a) and section 66(a) prohibit the disclosure of information affecting the life and physical safety of individuals.[220] The public interest override is applicable.[221] According to Currie and Klaaren "the ground is clearly intended to protect individuals from the possibility of harmful consequences as a result of revealing information about their identity, their personal history, their views or whereabouts and the like".[222] Evidently this exception protects the privacy of the individual concerned and is therefore of importance for data protection. (It also overlaps with the ground discussed in par *a* above.)

d Certain records of SARS

The information officer of the South African Revenue Services (SARS) must refuse a request for access to a record that contains information obtained for the purposes of enforcing legislation concerning the collection of revenue.[223] This ground for refusal is not subject to the public interest override. However, where the information relates to the requester (ie the data subject), the record may not be refused.[224] This provision allows a data subject access to his or her personal information despite a ground for refusal of access being present.

---

218 Currie & Klaaren *AIA commentary* 153 (par 8.58).

219 See par 4.2.7.1.

220 Currie & Klaaren *AIA commentary* 159 (par 8.69).

221 See par 4.2.7.1.

222 Currie & Klaaren *AIA commentary* 160 (par 8.70).

223 Act 2 of 2000 s 35(1).

224 Act 2 of 2000 s 35(2).

e Evaluative material held by public body

A public body may, *inter alia*, refuse access to a record held by the body if the record contains evaluative material, where the disclosure would jeopardise the effectiveness of the testing procedure, or where the disclosure would breach a promise made to the person who supplied the material to keep the material, or the identity of the person supplying it, confidential.[225] This provision protects the privacy of the person supplying evaluative material.

No parallel provision exists for evaluative material in the hands of private bodies. Currie and Klaaren submit that this is due to an oversight. The odd result of this, they point out, is that evaluative material produced by a private body (such as a personnel agency contracted by the government) is not protected on this ground in the hands of the private body. It is only protected once it has been delivered to a public body and an express or implied promise of confidentiality has been made.[226] (However, such material may be protected under par *a* above.)

4.2.8 Remedies: internal appeals and applications to court

4.2.8.1 Introduction

The AIA creates two mechanisms for the resolution of disputes and the reconsideration of decisions to grant or refuse access to information: internal appeals and judicial review.[227]

4.2.8.2 Internal appeals (public body)

225 Act 2 of 2000 s 44(2).

226 Currie & Klaaren *AIA commentary* 188 (par 8.104).

227 The early drafts of the Open Democracy Bill provided for specialised information courts and the creation of an Open Democracy Commission with powers of investigation.

In the case of certain public bodies,[228] requesters and third parties have the right to appeal against decisions of information officers.[229] A requester may appeal against a decision to refuse a request for access, to levy a fee, or to grant access in another form as requested. Third parties may appeal against a decision to grant access. The manner in which the appeal must be lodged and the fees payable are prescribed in detail in the Act.[230]

4.2.8.3 Applications to court

The Act makes provision for parties aggrieved by decisions of a public or private body regarding access to lodge an application to a court.[231] In the case of a public body, the internal appeal procedure must first be exhausted.[232]

A court hearing an application in terms of this Act may examine any record held by the body involved, but may not disclose the content of the record involved.[233] The court may receive *ex parte* applications,

228 Ie a public body as defined in part (a) of the definition - see fn 63.

229 Act 2 of 2000 s 74.

230 See Act 2 of 2000 s 75.

231 Act 2 of 2000 s 78(2). Currie & Klaaren*AIA commentary* 202 (par 9.9) ask the following questions regarding this application procedure, the answers to which are not evident from the Act: "Are the 'applications to court' provided for ... a form of statutory review of access decisions or are they appeals against them? On what grounds may one make an 'application to court' and on what grounds is the court justified in awarding the forms of relief listed...? Is the matter to be considered de novo, as it were a case of first impression or is the court confined to considering the 'record'?" They submit that, in the absence of specific indications in the Act, the applications to court procedure is best considered to permit a form of statutory judicial review of information decisions on grounds of lawfulness, reasonableness and procedural fairness.

232 Act 2 of 2000 s 78(1). The Act itself does not prescribe the rules of procedure for courts to follow, but provides that the Rules Board for Courts of Law must, subject to approval by Parliament, make and implement such rules within a year after the commencement of the Act (Act 2 of 2000 s 79). Before the implementation of such rules, applications must be lodged to a High Court (Act 2 of 2000 s 79(2)).

233 Act 2 of 2000 s 80(1) and 80(2). According to Govender "Limitation on access to information" 21, this section means "that in the final analysis the adequacy and logic of the reasons supplied can be directly tested by an objective and impartial body".

conduct hearings *in camera* and prohibit the publication of information relating to the proceedings.[234]

The court proceedings in terms of this Act are civil proceedings, and the burden of establishing that a decision complies with the provisions of the Act rests on the person alleging that it so complies.[235]

4.2.9 Offences

The Act makes it an offence to destroy, damage, alter, conceal or falsify a record with the intent to deny a right of access in terms of the Act.[236] A conviction may result in a fine or imprisonment for a period of not more than two years.[237] However, no person can be held liable for anything done in good faith in the exercise of powers in terms of the Act.[238]

4.2.10 Human Rights Commission

The Human Rights Commission is the body entrusted with oversight and the implementation of the Act.[239] However, the Human Rights Commission has no real authority or power over private or public bodies to enforce the provisions of the Act. Its functions are mainly to advise, assist, consult, make recommendations, submit reports, train persons, develop educational programmes, encourage participation or monitor compliance with the Act.[240]

---

234 Act 2 of 2000 s 80(3).

235 Act 2 of 2000 s 81.

236 This reflects the data protection principle of security (see ch 6 par 2.2.9).

237 Act 2 of 2000 s 90.

238 Act 2 of 2000 s 89.

239 The Human Rights Commission is the closest the Act comes to establishing a Data Protection Authority as encountered in the British Data Protection Act (see UK chap par 4.3.9.1) and the Netherlands Wet Bescherming Persoonsgegevens (see Neth chap par 4.3.11.1).

240 See Act 2 of 2000 s 83(2). Govender "Limitation on access to information" 25 describes the role of the Human rights Commission as "mentoring, monitoring and supervising".

The two most important functions of the Commission are that it must compile a guide on how to use the Act, and that it must annually submit a report to the National Assembly in which certain particulars regarding the implementation of the Act are given.[241]

All the other functions of the Commission are contingent on the financial and other resources available.[242] Expenditure by the Human Rights Commission in terms of this Act must be defrayed from moneys appropriated by Parliament to the Commission for that purpose.[243]

4.2.11 Summary

The AIA is essentially freedom of information legislation and is not primarily concerned with data protection, although it promotes data protection by permitting individuals access to personal information and by prohibiting access to third party information if this would lead to unreasonable infringement of the privacy of the third party.

These provisions embody, to some extent, the following data protection principles:

❒ data subject participation (by granting the individual access to his or her information, and, in an

241 Act 2 of 2000 s 83(1) and s 84. The report must include recommendations for the improvement of the Act, and particulars of the number or requests for access received, the number of requests granted (in full or partially), the number of requests refused and the number of times each provision of the Act was relied on to refuse access. The information officer of a public body must annually submit a report to the Human Rights Commission stating, *inter alia*, the number of requests for access received, granted in full, granted because the disclosure was in the public interest, refused in full or in part, and the number of internal appeals lodged because access was given or refused (Act 2 of 2000 s 32). According to Govender "Limitation on access to information" 26 "[t]he intention of this section is to provide a further measure of supervision at a general level of the different departments by both the Human Rights Commission and Parliament. This multifaceted approach seeks to ensure a reactive assessment of the correctness of the decision and an ongoing proactive appraisal of compliance with the Act with ultimate accountability to the legislature".

242 Act 2 of 2000 s 83(2).

243 Act 2 of 2000 s 85.

interim provision, by granting the individual a right to request correction of inaccurate data[244])

- disclosure limitation (by prohibiting access to third parties)

- openness (by requiring that an index of records should be kept)[245]

- accountability (by giving a requester the right to approach a court for a remedy in certain circumstances,[246] and by appointing the information officer or head of a private body as the person ultimately responsible for complying with the provisions of the Act)[247]

However, the AIA does not fulfil the data protection principles of purpose specification[248] and quality.[249] The fact that no real power is granted to the oversight body, namely the Human Rights Commission,[250] is a further serious shortcoming.

4.3 Open Democracy Bill

4.3.1 Introduction

The provisions of the Promotion of Access to Information Act discussed above originated in the Open

244 See par 4.2.3.3.

245 See par 4.2.5.

246 Together with the right to access and correction, this is known as the principle of data subject participation (see ch 6 par 2.2.6).

247 See par 4.2.4.

248 In regard to records of private bodies, the Act limits the right of access to information by requiring that the person who wants access should require the information for the protection of a right. See fn 116 and associated text.

249 See ch 6 par 2.2.

250 See par 4.2.10.

Democracy Bill (ODB).[251] However, as stated previously, not all the data privacy protection provisions of this Bill were included in the final Act. Those provisions that were omitted from the Act, but remain relevant for future legislation on this topic, will now be briefly considered.[252] The access provisions of the ODB will not be discussed, since they were implemented in the AIA.

4.3.2 Correction of personal information

When a person has been given access to his or her personal information by a private or government body in terms of the Bill, the person may ask for the correction of inaccurate information in the record.[253] This is an important provision, since it gives the data subject control over his or her image. False or inaccurate data infringe a person's right to identity and are in conflict with the data quality principle.[254]

Correction means amending, supplementing or deleting inaccurate information.[255] The request for correction must be made in the prescribed form or orally, and must specify the requester's contact information. The request must include enough particulars to enable the body to identify the record which contains the information which the requester considers to be inaccurate, and must specify in which respect the information is inaccurate.[256] Public bodies have a duty to assist requesters who are illiterate or have a disability, and must also transfer requests to the correct public body where the request was addressed to the wrong body.[257] Public bodies must also preserve records until a final decision on the

251 See par 4.2.1 and see Roos "Data protection" 43.

252 Also see Roos "Data protection" 43–48 for a discussion of the provisions of the ODB.

253 B 67–98 s 51(2) and 52(2).

254 See ch 6 par 2.2.4 and ch 7 par 2.3.2.1.b.

255 B 67–98 s 51(1) and 52(1).

256 B 67–98 s 51(5) and 52(5).

257 B 67–98 s 52(6) read with s 13(4), s 14 and s 15.

request for correction has been made.[258]

The head of the private body or the information officer of a government body must decide on the request within thirty days.[259] If the information officer of a government body fails to do so, this is regarded as a refusal of the request.[260]

If the head of a private body or the information officer of a government body decides that the information identified in the request for correction is incorrect, he or she must correct the information free of charge and send a copy of the correction to the requester. If the same information is contained in other records held by the body, the official must also correct those records.[261] In the case of a government body, the information officer must inform all other government bodies or persons to whom the inaccurate information has been supplied of the correction and inform the requester of each notice.[262] It is important that a data subject should be able to trace the third parties who have been supplied with the incorrect information so that the information can be corrected. For this purpose, data controllers should be under an obligation to keep a record of all third party transfers.

Where an inaccurate part of the information is to be deleted, a copy must first be made of that part and a note must be made on the original document that part of the information has been deleted. The copy must be kept as long as the record is kept.[263]

---

258 B 67–98 s 52(6) read with s 16.

259 B 67–98 s 51(6) and 52(7).

260 B 67–98 s 52(8).

261 B 67–98 s 51(7) and 52(9).

262 B 67–98 s 52(9)(c) and (d). The government body which has been supplied with inaccurate information must correct the information and notify the requester that it has been corrected, or, if it does not accept that the information is inaccurate, must make a note on the record to that effect and inform the requester of its decision. The requester may then lodge an internal appeal to decide the issue (see B 67–98 s 52(11)). A similar duty is not imposed on private bodies.

263 B 67–98 s 51(8) and 52(10).

If the head of the private body or the information officer of the government body decides that the information is not inaccurate, and provided the request was not irrelevant, frivolous or vexatious, a notice must be attached to the record indicating that the person disputes the accuracy of the information. The requester must be informed of the decision and be given a copy of the notice.[264] In the case of a government body, the requester has another opportunity to make a statement giving reasons why he or she thinks that the information is inaccurate, which statement must also be attached to the record containing the disputed information. The requester may also lodge an internal appeal against the decision not to correct the information.[265]

Any disclosure or use of a record after it has been corrected, or after a note or statement has been attached to it, must be in its corrected form or must include the note or statement.[266]

4.3.3 Use and disclosure of personal information

In general, personal information may not be used or disclosed without the consent of the person concerned, except for specific purposes mentioned in the Bill.[267] This provision is in accordance with the principle that data processing can only take place lawfully if there is a ground of justification present, such as consent or a legitimate private or public interest.[268] This provision also reflects aspects of the data protection principles of fair and lawful processing, purpose specification and disclosure limitation.[269] The person's consent must be obtained in a prescribed manner and form and may be withdrawn at a later stage.[270]

264 B 67–98 s 51(11) and 52(12)

265 B 67–98 s 52(12).

266 B 67–98 s 51(10) and (11) and s 52(13) and (14).

267 B 67–98 s 53, s 54, s 55 and s 56.

268 See ch 7 par 2.3.2.3.

269 See ch 6 par 2.2.

270 B 67–98 s 58. This is in accordance with the principle that consent can never be given irrevocably, because
(continued...)

Private and government bodies may use and disclose personal information for the purpose for which it was originally compiled, or for a purpose consistent with that purpose.[271] A purpose will be consistent with the original purpose if the person to whom the information relates and from whom it was originally collected might reasonably have expected such a use or disclosure.[272]

Personal information may also be used by private and government bodies for a purpose for which the information may be disclosed to that body in terms of the Bill.[273]

Private and government bodies may furthermore disclose personal information on one of the following grounds:[274]

- ❒ in accordance with the Open Democracy Bill[275] or any other law that authorises the disclosure
- ❒ to comply with a subpoena, warrant, court order or rules of court relating to the production of information
- ❒ for the purpose of avoiding prejudice to the maintenance of the law, including the prevention, detection, prosecution and punishment of an offence
- ❒ for the purpose of averting or lessening an imminent and serious threat to the health or safety of an individual or the public

270(...continued)
it is *contra bonos mores* (see ch 7 par 2.3.2.3).

271 B 67–98 s 53(a) and (b); s 54(a) and (b).

272 B 67–98 s 57.

273 Ie in terms of B 67–98 s 55 or 56 (see B 67–98 s 53(c) and 54(c)).

274 B 67–89 s 55 and 56.

275 Ie B 67–89 s 50 and Part 3.

- for the purpose of the performance of a contract to which the person to whom the information relates is a party

- for any prescribed purpose which would not pose a threat to the privacy of the person to whom the information relates, where the person (when consulted by the body) did not object to the disclosure, or where the disclosure is necessary to further the legitimate interests of the private or public body

Public bodies have more extensive grounds for the disclosure of personal information than private bodies. Apart from the grounds already mentioned, government bodies may also disclose information on the following grounds:

- to a prosecuting authority for the purposes of criminal proceedings or to a legal practitioner representing the state, the government, a governmental official or a government body in civil proceedings for the purposes of those civil proceedings

- to a government body, on the written request of that body, for the purposes of enforcing the law or carrying out an investigation in terms of the law, if the request specifies the purposes and describes the information to be disclosed

- in terms of an agreement between the government of South Africa and the government of a foreign state or an international organisation, for the purposes of law enforcement or carrying out an investigation in terms of the law

- to an official of a government body for the purpose of an internal audit, or to the Auditor General's office for the purpose of an audit or to a person appointed to carry out an audit in respect of a government body

- to an archives repository in accordance with the relevant legislation

- to any person for research or statistical purposes if there are reasonable grounds to believe that the purpose for which the information is disclosed could not reasonably be accomplished unless the information is provided in a form that would identify the person to whom the information relates, and the information officer obtains an undertaking from the person that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the person to whom or which it relates

- to a government body for the purposes of locating a person to collect a debt owing to the state or to pay a debt owed by the State

The sections relating to the use and disclosure of records will not immediately apply to records held before the commencement of the Bill, but a period will be specified by regulation in which the government or private body will be given an opportunity to obtain the consent of the persons to whom the personal information relates.[276]

In terms of the Open Democracy Bill, the index of records held by the government body must include a statement of the purposes for which the information was obtained as well as a statement of the purposes consistent with those purposes.[277] This provision enables the data subject to learn the purpose of the data processing, and is an attempt to give effect to the principles of openness and purpose specification of data protection.[278]

If the use or purpose of personal information is not included in these statements, the head of the government body must keep a register of any use or disclosure of that personal information and attach

276 B 67–98 s 59. The consent need not in actual fact be given. If the prescribed steps have been taken to obtain the consent, the person will be considered to have consented whether or not that person in fact gave consent (B 67– 98 s 59(2)). However, such consent may be withdrawn as prescribed (B 67– 98 s 59(3)).

277 B 67–98 s 6(2)(d).

278 See ch 6 par 2.2.

that register to the personal information.[279] The register will then be considered to form part of the personal information to which it is attached.[280] If the personal information is used or disclosed for a purpose consistent with the purpose for which it was obtained or compiled, but the use is not included in the statement of compatible uses, the head of the body must ensure that the use is included in the next manual that is published.[281]

Lastly, it should be noted that the Bill excludes certain information from the provisions regarding the use and disclosure of personal information, namely information already publicly available, or created or acquired and preserved solely for public reference or exhibition purposes in a library or museum, or placed by a person other than the government in an archives repository or a library or museum controlled by a government body, or where the information relates to an individual who is or was an official of a government body if the information relates to the position or functions of the official.[282] The rationale for these exclusions is either that privacy is not infringed, or that a legitimate ground of justification is present.

4.3.4 Collection of personal information (public bodies)

The Open Democracy Bill contains provisions regarding the collection of personal information, but only with regard to government bodies. The collection of information by private bodies is left unregulated. This is an important omission which should be rectified.

In terms of the Bill, a government body may not collect information unless such collection is required or permitted in terms of legislation or required for the performance of the functions of the body;[283] in

279 B 67–98 s 60(1).

280 B 67–98 s 60(2).

281 B 67–98 s 60(3).

282 B 67–98 s 48.

283 B 67–98 s 61(1). This provision complies with the data protection principles of fair and lawful processing (continued...)

other words the collection of data must be justified by the presence of a legitimate public interest. A government body must also, if this is reasonably possible, collect personal information directly from the person involved where such personal information is intended to be or may be used in taking any decision which affects a person's right or determines the content of the right. Where this is done, the data subject is aware of the fact that data have been or are being collected, and the content of the data can be better controlled. Two exceptions are made to this rule: where the person has authorised the body to collect the information from someone else, or where the government body may get the information from another government body in terms of the provisions allowing for disclosure of personal information by a government body.[284]

When information is collected directly from a person, the person must be informed for what purpose the information is being collected, for whom it is being collected, by whom it will be held, whether it is being collected in terms of legislation permitting the collection, and if so, whether it is compulsory to supply the information or not. The person must also be informed about his or her right of access to information held by the body and of the right to ask for correction of personal information.[285] Correction means amending or supplementing information or deleting inaccurate information.[286] These provisions reflect various data protection principles, such as fair and lawful processing, purpose specification, openness and data subject participation.[287]

If the collection of information directly from the person would defeat the purpose or prejudice the use for which the information is being collected, the requirement does not apply.[288]

283(...continued)
and purpose specification (see ch 6 par 2.2).

284 Ie in terms of B 67–98 s 56 (see B 67–98 s 61(2)).

285 Ie in terms of B 67–98 s 9 and s 52 (see B 67–98 s 61(3)).

286 B 67-98 s 51(1) & 52(1).

287 See ch 6 par 2.2.

288 B 67–98 s 61(4).

The Bill also excludes from the provisions regarding the collection of personal information the following personal information: information which is already publicly available, or which has been created or acquired and preserved solely for public reference or for purposes of exhibition in a library or museum, or which has been placed by a person other than the government in an archives repository or a library or museum controlled by a government body, or information that concerns an individual who is or was an official of a government body if the information relates to the position or functions of the official.[289]

4.3.5 Retention, accuracy and disposal of personal information (public bodies)

The head of a government body must take responsibility for the security and confidentiality of personal information kept by the body.[290] The head is also responsible for ensuring that personal information which is used when making a decision that affects a person's right or determines the content of that right should be accurate, up-to-date and as complete as possible.[291] By assigning responsibility for data protection to the head of the body, government emphasises the importance of data protection. These provisions also reflect the data protection principle of accountability.[292] Once the information has been used, it must be kept for a prescribed period to ensure that the person to whom it relates has a reasonable opportunity to obtain access to the information,[293] and it may only be disposed of by the head of the department in a prescribed manner.[294]

Again, the Bill excludes from the above-mentioned provisions personal information already publicly available, or created or acquired and preserved solely for public reference or exhibition purposes in a

289 B 67–98 s 48.

290 This reflects the accountability principle (see ch 6 par 2.2.10, ch 7 par 5) and the data protection principle of security (see ch 6 par 2.2.9).

291 B 67–98 s 62(2). Compare also the data protection principle of data quality. See ch 6 par 2.2.

292 See ch 6 par 2.2.

293 B 67–98 s 62(1).

294 B 67–98 s 62(3).

library or museum, or placed by a person other than the government in an archives repository or a library or museum controlled by a government body, or information that relates to an individual who is or was an official of a government body if the information relates to the position or functions of the official.[295]

4.3.6 Summary

When the ODB is measured against the data protection principles,[296] it becomes apparent that the ODB has attempted to comply with the data protection principle of data subject participation. This principle requires *inter alia* that data subjects should be able to request the correction of inaccurate information concerning themselves.[297] However, a shortcoming in these provisions is the fact that whereas public bodies must inform all other government bodies or persons to whom inaccurate information has been supplied of a subsequent correction of such information,[298] private bodies are not under a similar obligation.

As regards the collection of personal data, the Bill protects the individual only when the personal information at issue has been collected by the public sector. Similar protection is not provided for the private sector. This serious shortcoming should be addressed. The provisions of the Bill regarding the collection of data should furthermore be improved, by explicitly stating that the purpose for which the information is collected should be a legitimate purpose, in order to comply with the purpose specification principle and to ensure that processing takes place lawfully.[299] Another shortcoming is that the ODB does not make specific provision for sensitive information, direct marketing or automated

295 B 67–98 s 48.

296 See ch 6 par 2.2 where all the principles are discussed.

297 See par 4.3.2 and on the principle of data subject participation see ch 6 par 2.2.6.

298 See fn 262.

299 See par 4.3.4.

decision making.[300]

The Bill contains provisions reflecting the data protection principles of purpose specification and disclosure limitation, since it clearly provides that personal information may not be used or disclosed without the consent of the individual concerned, except for specific purposes mentioned in the Bill.[301]

The data quality principle is reflected in regard to public bodies, since the Bill provides that the data should be accurate, up-to-date and complete. This provision can be improved by requiring that the information should be relevant to and necessary for the purpose for which it is collected and used and by extending the provision to private bodies.

The principles of security and accountability are also reflected in the Bill, but only in regard to public bodies.[302] It is submitted that private bodies should also be under a specific obligation to nominate a person to be responsible for the security of personal information. The Bill could be improved by imposing a duty of confidentiality on data controllers and processors.

In conclusion, the provisions of the ODB, with the suggested amendments, could profitably be used as guidelines when drawing up data protection legislation for South Africa.

4.4 Electronic Communications and Transactions Act

4.4.1 Introduction

In the Green Paper on Electronic Commerce for South Africa (Theme 2 "Building trust in the electronic

300 See the principle of sensitivity (ch 6 par 2.2.8).

301 See par 4.3.3 and ch 6 par 2.2.2 and 2.2.5.

302 See par 4.3.5.

economy")[303] it was emphasised that the growth and development of electronic commerce relies on building the confidence of the consumer in the electronic commerce environment. Lack of privacy is a major concern for individuals in the use of the electronic medium in commerce.[304] Any act introduced to regulate electronic commerce should therefore address this concern. Chapter VIII of the Electronic Communications and Transactions Act (ECTA)[305] aims to address consumers'[306] privacy concerns.

4.4.2 Scope of protection

The protection of personal information[307] in the ECTA only applies to personal information –

- ❒ on natural persons,[308]
- ❒ that has been obtained through electronic transactions,
- ❒ after the introduction of the Act.[309]

303 See http://www.ecomm-debate.co.za/greenpaper/theme2.htm

304 "This includes not only the privacy of the communication between the parties in a transaction eg the protection of credit and debit card numbers while traversing the Internet, or of other personal details, which can be solved through the use of encryption; but also the accumulation of personal data at Websites visited, for example through the use of "cookies" or the introduction of Customer Relationship Management Tools (CRMs). In the nature of any distance-contract, the supplying party must collect a certain amount of personal information, even if this is only the name and address, and the credit card number, of the buyer. However, it is possible ... that information of a much more personal nature, such as race, health, financial standing, sexual orientation, is collected, frequently without any indication of how this information is subsequently to be used. In particular, the disclosure of such information to other parties must be controlled, if not prevented altogether"(Green Paper on Electronic Commerce for South Africa – Theme 2 "Building trust in the electronic economy" par 8.3).

305 Act 25 of 2002. For an overview of the Act, see Jansen 2002 (Apr) *De Rebus* 17.

306 Act 25 of 2002 s 1 defines a "consumer" as "any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier".

307 The definition of personal information given in s 1 of the ECTA is exactly the same as that of the AIA (see fn 200 above).

308 As pointed out in regard to the AIA as well, this is a shortcoming in the Act, since South African law recognises a right to privacy in respect of juristic persons. See ch 7 par 2.5.2.

309 Act 25 of 2002 s 50(1) read with the definition of "data subject" in s 1("data subject means any natural person from or in respect of whom personal information has been requested, collected, collated, processed or stored, after the commencement of this Act").

However, the Act does not impose legally binding obligations on data controllers.[310] The ECTA enumerates principles that must be adhered to when a data controller electronically collects personal information,[311] but provides that "a data controller may voluntarily subscribe to the principles ... by recording such fact in any agreement with a data subject".[312] The data subject and the data controller must therefore reach an agreement that the data controller will adhere to these principles, before they will become applicable to the transaction between the data subject and the data controller. The rights and obligations of the parties in respect of the breach of the principles are governed by the terms of any agreement between them.[313] The Act further provides that a data controller must subscribe to all the principles and not merely to parts thereof.[314]

4.4.3 Principles for electronic processing of personal information

Although the header to the relevant section of the Act refers only to the collection of information, the principles themselves also deal with the collation, processing, storage and disclosure of the data. However, the ECTA does not regulate access to information – the provisions of the AIA are applicable in this regard.[315]

Section 51 lists nine principles that data controllers should adhere to when processing personal information:

The first principle requires the express written consent of the data subject before the data controller

310 Act 25 of 2002 s 1 defines data controllers as "any person who electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject".

311 Act 25 of 2002 s 51.

312 Act 25 of 2002 s 50(2).

313 Act 25 of 2002 s 50(4).

314 Act 25 of 2002 s 50(3).

315 See par 4.2.3.1.

may collect, collate, process or disclose personal information on the data subject.[316] Since such consent must be expressly given, it follows that consent may not be implied from the conduct of a person. For example, the failure of a person to respond to a request by the data controller to use the personal information collected cannot be construed as consent to such a request. Presumably, consent given electronically (eg by ticking a box on a web page) will also qualify as written consent. One of the objects of the ECTA is to "enable and facilitate electronic communications and transactions in the public interest"[317] and it would therefore be counterproductive to require written consent in paper form. Consent is, however, not required where the data controller is permitted or required by law to process data. This would include situations where data processing takes place for the maintenance and furtherance of legitimate private and public interests.[318]

The second principle provides that the data requested, collected, collated, processed or stored by a data controller must be necessary for the lawful purpose(s) for which the personal information is required.[319] This principle emphasises that the data controller must have a lawful purpose for the processing of personal information and that the data processing must be necessary for that purpose. As was previously indicated, data processing can have a lawful purpose only if the object is to further or protect a legitimate interest.[320] A legitimate interest in the e-commerce environment would for example be that a data controller (such as a supplier of products) needs the name and address of the data subject (eg a buyer of goods) to deliver the products and to send out a bill – in short, a legitimate commercial interest.

The third principle states that the data controller must disclose in writing to the data subject the

3160 Act 25 of 2002 s 51(1). This is in accordance with the principle that processing should take place lawfully and with the data protection principle of openness, which requires that the data subject should know about the data processing (see ch 6 par 2.2.7 and ch 7 par 4.2.1).

317 Act 25 of 2002 s 2(1).

318 See ch 7 par 2.3.2.3.c.

319 This contains elements of the data protection principles of purpose specification and minimality (see ch 6 par 2.2.2 and 2.2.3).

320 See ch 7 par 2.3.2.3.c.

specific purpose(s) for which any personal information is being requested, collected, collated, processed or stored. Without such knowledge it would be very difficult for the data subject to judge whether or not the processing of data was lawful – in other words, whether a legitimate interest is being protected and whether the data processed are necessary for this purpose.[321]

The fourth principle provides that a data controller may not use the personal information for any other purpose than the disclosed purpose without the express written permission of the data subject, unless he or she is permitted or required to do so by law. This principle echoes the first principle. Presumably, the aim of this provision is to regulate the further use (secondary use) of the information. It would have been better to have formulated this principle in terms similar to the second principle of the UK Data Protection Act, which requires that personal data must be obtained only for one or more specified and lawful purposes, and may not be further processed in any manner that is incompatible with such purpose or purposes.[322] According to such a formulation, as long as the secondary use is compatible with the original purpose, the processing is lawful. As the fourth principle is formulated at present, compatible use is not allowed without the express written consent of the data subject.

The fifth principle requires the data controller to keep a record of the personal information and the specific purpose for which the personal information was collected, for as long as the personal information is used and for a period of at least one year thereafter. It is unclear why the information should be kept for one year. The usual requirement is that personal data processed for any purpose or purposes may not be kept for longer than is necessary for such purpose or purposes.[323]

According to the **sixth principle**, a data controller may not disclose any of the personal information

321 This is once again a reflection of the data protection principle of purpose specification (see ch 6 par 2.2.2) and the principle of openness, which requires that the data subject must have a knowledge of the purpose of data processing (see ch 6 par 2.2.7 and ch 7 par 4.2.2).

322 See ch 4 par 4.3.4.3.

323 See ch 4 par 4.3.4.3.

held by it to a third party,[324] unless required or permitted by law or specifically authorised to do so in writing by the data subject. This reflects the data protection principle of disclosure limitation.[325]

The **seventh principle** relates to the fifth principle – the data controller must, for as long as the personal information is used and for a period of at least one year thereafter, keep a record of any third party to whom the personal information was disclosed and of the date on which and the purpose for which it was disclosed. Knowledge of third party access is an active control principle of data protection.[326] If a data subject knows for example that personal information transferred to third parties is inaccurate, he or she would be able to correct the transferred information in the hands of the third parties.[327]

Principle eight requires the data controller to delete or destroy all personal information which has become obsolete.[328] The purpose for which the data are processed plays a role in determining whether the information is obsolete. Data are obsolete if they are no longer necessary for the purpose for which they were collected.[329] This active control principle should be extended to the correction or deletion of inaccurate data.[330] However, the ECTA contains no provisions regarding such correction or deletion

---

324 A third party is defined in Act 25 of 2002 s 1 as "in relation to a service provider ... a subscriber to the service provider's services or any other user of the service provider's services or a user of information systems".

325 See ch 6 par 2.2.5.

326 See ch 7 par 4.2.4.

327 Note, however, that the ECTA does not provide for the correction of inaccurate data. Recourse can be had to the AIA, which provides for access to information and provides that if a provision for the correction of personal information in a record held by a public or private body does not exist, that body must take reasonable steps to establish adequate and appropriate internal measures providing for such correction until legislation providing for such correction takes effect (see par 4.2.3.3).

328 The fact that data are obsolete affects the quality of the data (see ch 6 par 2.2.4).

329 This is a reflection of the principles of minimality and data quality (see ch 6 par 2.2).

330 See ch 7 par 4.2.5; ch 6 par 2.2.6; ch 4 par 4.3.4.5.

– the AIA deals with the correction of personal information, albeit as a transitional measure only.[331] Presumably the expectation is that the envisaged data protection legislation will address this issue.[332]

The **ninth principle** permits the data controller to use the personal information to compile profiles for statistical purposes and to freely trade with such profiles and statistical data, as long as the profiles or statistical data cannot be linked to any specific data subject by a third party. It is a generally accepted principle that data processing may take place for statistical purposes, provided that the anonymity of data subjects is ensured.[333]

4.4.4 Summary

The ECTA is a first attempt to provide for data protection principles in the electronic commerce environment. However, it does not impose binding obligations on data controllers. The parties involved have to make the principles applicable by means of the contract between them. Since adherence to these principles will probably impose an economic burden on data controllers, they will not be eager to contract on this basis. It remains to be seen whether these principles will be implemented in practice.

5 CONCLUSION

The right to privacy is recognised and protected in private law and in the Constitution.[334] This constitutional imperative obliges the government to adopt legislation for the adequate protection of data privacy, since ordinary private law principles provide only partial protection in this respect.[335] The AIA, ODB and ECTA can all be considered to be first steps in the right direction, but not to be complete

331 See fn 327.

332 See par 4.2.1.

333 See ch 7 par 2.3.2.c.ii.

334 See ch 7 par 2.3.2.1.a.

335 See ch 7 par 3.1.

solutions. Legislation incorporating internationally accepted data protection principles[336] is therefore necessary[337] and is expected to be passed.[338]

For more than two decades, South African writers have campaigned for data protection legislation.[339] It is to be welcomed that the necessity of such legislation has finally been accepted, and all that remains is to implement an effective data protection regime.

336 See chap 6 par 1.3.2.3.

337 Also see the conclusions drawn from the comparative study in this regard (chap 6 par 1.1).

338 See par 4.2.1 above.

339 See Neethling *Privaatheid* 406; 1980 *THRHR* 141, 155; "Databeskerming" 105 *et seq;* McQuoid-Mason *Privacy* 195 *et seq*; Eiselen *Reg op privaatheid in die inligtingsera* par 7; Roos 1990 *TSAR* 264, 265; Schulze 1994 *THRHR* 75, 85–86; Burns *Communications law* 201.