Government Gazette

REPUBLIC OF SOUTH AFRICA

Vol. 581 Cape Town 26 November 2013 No. 37067

THE PRESIDENCY

No. 912 26 November 2013

It is hereby notified that the President has assented to the following Act, which is hereby published for general information:–

No. 4 of 2013: Protection of Personal Information Act, 2013.

GENERAL EXPLANATORY NOTE:

[ ] Words in bold type in square brackets indicate omissions from existing enactments.

Words underlined with a solid line indicate insertions in existing enactments.

(English text signed by the President)
(Assented to 19 November 2013)

ACT

To promote the protection of personal information processed by public and private bodies; to introduce certain conditions so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Regulator to exercise certain powers and to perform certain duties and functions in terms of this Act and the Promotion of Access to Information Act, 2000; to provide for the issuing of codes of conduct; to provide for the rights of persons regarding unsolicited electronic communications and automated decision making; to regulate the flow of personal information across the borders of the Republic; and to provide for matters connected therewith.

PREAMBLE

RECOGNISING THAT—

- section 14 of the Constitution of the Republic of South Africa, 1996, provides that everyone has the right to privacy;
- the right to privacy includes a right to protection against the unlawful collection, retention, dissemination and use of personal information;
- the State must respect, protect, promote and fulfil the rights in the Bill of Rights;

AND BEARING IN MIND THAT—

- consonant with the constitutional values of democracy and openness, the need for economic and social progress, within the framework of the information society, requires the removal of unnecessary impediments to the free flow of information, including personal information;

AND IN ORDER TO—

- regulate, in harmony with international standards, the processing of personal information by public and private bodies in a manner that gives effect to the right to privacy subject to justifiable limitations that are aimed at protecting other rights and important interests,

PARLIAMENT of the Republic of South Africa therefore enacts, as follows:—

CONTENTS OF ACT

Condition 6

Openness

Condition 7

Security safeguards

Condition 8

Data subject participation

Part B

Processing of special personal information

Part C

Processing of personal information of children

CHAPTER 4

EXEMPTION FROM CONDITIONS FOR PROCESSING OF PERSONAL INFORMATION

CHAPTER 5

SUPERVISION

Part A

Information Regulator

CHAPTER 9

TRANSBORDER INFORMATION FLOWS

CHAPTER 10

ENFORCEMENT

CHAPTER 11

OFFENCES, PENALTIES AND ADMINISTRATIVE FINES

CHAPTER 12

GENERAL PROVISIONS

SCHEDULE

Laws amended by section 110

CHAPTER 1

DEFINITIONS AND PURPOSE

Definitions

1. In this Act, unless the context indicates otherwise—

"biometrics" means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition;

"child" means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself;

"code of conduct" means a code of conduct issued in terms of Chapter 7;

"competent person" means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child;

"consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

"Constitution" means the Constitution of the Republic of South Africa, 1996;

"data subject" means the person to whom personal information relates;

"de-identify", in relation to personal information of a data subject, means to delete any information that—

(a) identifies the data subject;

(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject,

and **"de-identified"** has a corresponding meaning;

"direct marketing" means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of—

(a) promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or

(b) requesting the data subject to make a donation of any kind for any reason;

"electronic communication" means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient;

"enforcement notice" means a notice issued in terms of section 95;

"filing system" means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;

"information matching programme" means the comparison, whether manually or by means of any electronic or other device, of any document that contains personal information about ten or more data subjects with one or more documents that contain personal information of ten or more data subjects, for the purpose of producing or verifying information that may be used for the purpose of taking any action in regard to an identifiable data subject;

"information officer" of, or in relation to, a—

(a) public body means an information officer or deputy information officer as contemplated in terms of section 1 or 17; or

(b) private body means the head of a private body as contemplated in section 1, of the Promotion of Access to Information Act;

"Minister" means the Cabinet member responsible for the administration of justice;

"operator" means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party;

"person" means a natural person or a juristic person;

"personal information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

(a) information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

(b) information relating to the education or the medical, financial, criminal or employment history of the person;

(c) any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

(d) the biometric information of the person;

(e) the personal opinions, views or preferences of the person;

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

(g) the views or opinions of another individual about the person; and

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

"prescribed" means prescribed by regulation or by a code of conduct;

"private body" means—

(a) a natural person who carries or has carried on any trade, business or profession, but only in such capacity;

(b) a partnership which carries or has carried on any trade, business or profession; or

(c) any former or existing juristic person, but excludes a public body;

"processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

(a) the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

(b) dissemination by means of transmission, distribution or making available in any other form; or

(c) merging, linking, as well as restriction, degradation, erasure or destruction of information;

"professional legal adviser" means any legally qualified person, whether in private practice or not, who lawfully provides a client, at his or her or its request, with independent, confidential legal advice;

"Promotion of Access to Information Act" means the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000);

"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;

"public record" means a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body;

"record" means any recorded information—

(a) regardless of form or medium, including any of the following:

(i) Writing on any material;

(ii) information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;

(iii) label, marking or other writing that identifies or describes any thing of which it forms part, or to which it is attached by any means;

(iv) book, map, plan, graph or drawing;

(v) photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced;

(b) in the possession or under the control of a responsible party;

(c) whether or not it was created by a responsible party; and

(d) regardless of when it came into existence;

"Regulator" means the Information Regulator established in terms of section 39;

"re-identify", in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that—

(a) identifies the data subject;

(b) can be used or manipulated by a reasonably foreseeable method to identify the data subject; or

(c) can be linked by a reasonably foreseeable method to other information that identifies the data subject,

and **"re-identified"** has a corresponding meaning;

"Republic" means the Republic of South Africa;

"responsible party" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

"restriction" means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information;

"special personal information" means personal information as referred to in section 26;

"this Act" includes any regulation or code of conduct made under this Act; and

"unique identifier" means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

Purpose of Act

2. The purpose of this Act is to—

(a) give effect to the constitutional right to privacy, by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at—

(i) balancing the right to privacy against other rights, particularly the right of access to information; and

(ii) protecting important interests, including the free flow of information within the Republic and across international borders;

(b) regulate the manner in which personal information may be processed, by establishing conditions, in harmony with international standards, that prescribe the minimum threshold requirements for the lawful processing of personal information;

(c) provide persons with rights and remedies to protect their personal information from processing that is not in accordance with this Act; and

(d) establish voluntary and compulsory measures, including the establishment of an Information Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.

CHAPTER 2

APPLICATION PROVISIONS

Application and interpretation of Act

3. (1) This Act applies to the processing of personal information—

(c) samesmelting, koppeling, asook inperking, degradasie, uitwissing of vernietiging van inligting;

"Reguleerder" die Inligtingsreguleerder ingevolge artikel 39 ingestel;

"rekord" enige opgetekende inligting—

(a) ongeag vorm of medium, met inbegrip van enige van die volgende:
- (i) Skrif op enige materiaal;
- (ii) inligting geproduseer, opgeteken of gestoor by wyse van enige bandopnemer, rekenaartoerusting, hetsy hardeware of sagteware of beide, of ander toestel, en enige materiaal vervolgens verkry uit die inligting aldus geproduseer, opgeteken of gestoor;
- (iii) etiket, merk, of ander skrif wat enige voorwerp waarvan dit deel uitmaak, of waaraan dit op enige wyse geheg is, identifiseer of beskryf;
- (iv) boek, kaart, plan, grafiek of tekening;
- (v) foto, film, negatief, band of ander toestel waarin een of meer visuele beelde vervat is sodat dit geskik is, met of sonder die hulp van ander toerusting, vir reproduksie;

(b) in die besit of onder die beheer van 'n verantwoordelike party;

(c) hetsy dit deur die verantwoordelike party geskep is al dan nie; en

(d) ongeag wanneer dit tot stand gekom het;

"Republiek" die Republiek van Suid-Afrika;

"spesiale persoonlike inligting" persoonlike inligting soos by artikel 26 bedoel;

"toestemming" enige vrywillige, bepaalde en ingeligte wilsuitdrukking ingevolge waarvan verlof tot die prosessering van persoonlike inligting gegee word;

"unieke identifiseerder" enige identifiseerder wat aan 'n datasubjek toegewys word en wat deur 'n verantwoordelike party vir doeleindes van die bedrywighede van daardie verantwoordelike party gebruik word en waarmee daardie verantwoordelike party die datasubjek op unieke wyse identifiseer;

"verantwoordelike party" 'n openbare of privaatliggaam of enige ander persoon wat, eiehandig of in samewerking met andere, die oogmerk van en middele van prosessering van persoonlike inligting bepaal;

"voorgeskryf" voorgeskryf by regulasie of by 'n gedragskode; en

"Wet op Bevordering van Toegang tot Inligting" die Wet op Bevordering van Toegang tot Inligting, 2000 (Wet No. 2 van 2000).

Oogmerk van Wet

2. Die oogmerk van hierdie Wet is om—

(a) gevolg te gee aan die grondwetlike reg op privaatheid, deur persoonlike inligting te beskerm wanneer dit deur 'n verantwoordelike party geprosesseer word, onderhewig aan regverdigbare beperkings wat gerig is op die—
- (i) balansering van die reg op privaatheid teenoor ander regte, in besonder die reg op toegang tot inligting; en
- (ii) beskerming van belangrike belange, met inbegrip van die vrye vloei van inligting binne die Republiek en oor internasionale grense;

(b) die wyse waarop persoonlike inligting geprosesseer mag word, te reguleer deur voorwaardes, in harmonie met internasionale standaarde, te vestig wat die minimum vereistes vir die regmatige prosessering van persoonlike inligting voorskryf;

(c) persone van regte en remedies te voorsien ten einde hul persoonlike inligting teen prosessering wat nie in ooreenstemming met hierdie Wet is nie, te beskerm; en

(d) vrywillige en verpligte maatreëls, met inbegrip van die instelling van 'n Inligtingsreguleerder, in te stel, ten einde respek vir, en die bevordering, afdwinging en verwesenliking van, die regte wat in hierdie Wet beskerm word, te verseker.

HOOFSTUK 2

TOEPASSINGSBEPALINGS

Toepassing en uitleg van Wet

3. (1) Hierdie Wet is van toepassing op die prosessering van persoonlike inligting—

(a) entered in a record by or for a responsible party by making use of automated or non-automated means: Provided that when the recorded personal information is processed by non-automated means, it forms part of a filing system or is intended to form part thereof; and

(b) where the responsible party is—

(i) domiciled in the Republic; or

(ii) not domiciled in the Republic, but makes use of automated or non-automated means in the Republic, unless those means are used only to forward personal information through the Republic.

(2) *(a)* This Act applies, subject to paragraph *(b)*, to the exclusion of any provision of any other legislation that regulates the processing of personal information and that is materially inconsistent with an object, or a specific provision, of this Act.

(b) If any other legislation provides for conditions for the lawful processing of personal information that are more extensive than those set out in Chapter 3, the extensive conditions prevail.

(3) This Act must be interpreted in a manner that—

(a) gives effect to the purpose of the Act set out in section 2; and

(b) does not prevent any public or private body from exercising or performing its powers, duties and functions in terms of the law as far as such powers, duties and functions relate to the processing of personal information and such processing is in accordance with this Act or any other legislation, as referred to in subsection (2), that regulates the processing of personal information.

(4) **"Automated means"**, for the purposes of this section, means any equipment capable of operating automatically in response to instructions given for the purpose of processing information.

Lawful processing of personal information

4. (1) The conditions for the lawful processing of personal information by or for a responsible party are the following:

(a) "Accountability", as referred to in section 8;

(b) "Processing limitation", as referred to in sections 9 to 12;

(c) "Purpose specification", as referred to in sections 13 and 14;

(d) "Further processing limitation", as referred to in section 15;

(e) "Information quality", as referred to in section 16;

(f) "Openness", as referred to in sections 17 and 18;

(g) "Security safeguards", as referred to in sections 19 to 22; and

(h) "Data subject participation", as referred to in sections 23 to 25.

(2) The conditions, as referred to in subsection (1), are not applicable to the processing of personal information to the extent that such processing is—

(a) excluded, in terms of section 6 or 7, from the operation of this Act; or

(b) exempted in terms of section 37 or 38, from one or more of the conditions concerned in relation to such processing.

(3) The processing of the special personal information of a data subject is prohibited in terms of section 26, unless the—

(a) provisions of sections 27 to 33 are applicable; or

(b) Regulator has granted an authorisation in terms of section 27(2),

in which case, subject to section 37 or 38, the conditions for the lawful processing of personal information as referred to in Chapter 3 must be complied with.

(4) The processing of the personal information of a child is prohibited in terms of section 34, unless the—

(a) provisions of section 35(1) are applicable; or

(b) Regulator has granted an authorisation in terms of section 35(2),

in which case, subject to section 37, the conditions for the lawful processing of personal information as referred to in Chapter 3 must be complied with.

(5) The processing of the special personal information of a child is prohibited in terms of sections 26 and 34 unless the provisions of sections 27 and 35 are applicable in which

case, subject to section 37, the conditions for the lawful processing of personal information as referred to in Chapter 3 must be complied with.

(6) The conditions for the lawful processing of personal information by or for a responsible party for the purpose of direct marketing by any means are reflected in Chapter 3, read with section 69 insofar as that section relates to direct marketing by means of unsolicited electronic communications.

(7) Sections 60 to 68 provide for the development, in appropriate circumstances, of codes of conduct for purposes of clarifying how the conditions referred to in subsection (1), subject to any exemptions which may have been granted in terms of section 37, are to be applied, or are to be complied with within a particular sector.

Rights of data subjects

5. A data subject has the right to have his, her or its personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in Chapter 3, including the right—

(a) to be notified that—
  (i) personal information about him, her or it is being collected as provided for in terms of section 18; or
  (ii) his, her or its personal information has been accessed or acquired by an unauthorised person as provided for in terms of section 22;
(b) to establish whether a responsible party holds personal information of that data subject and to request access to his, her or its personal information as provided for in terms of section 23;
(c) to request, where necessary, the correction, destruction or deletion of his, her or its personal information as provided for in terms of section 24;
(d) to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information as provided for in terms of section 11(3)*(a)*;
(e) to object to the processing of his, her or its personal information—
  (i) at any time for purposes of direct marketing in terms of section 11(3)*(b)*; or
  (ii) in terms of section 69(3)*(c)*;
(f) not to have his, her or its personal information processed for purposes of direct marketing by means of unsolicited electronic communications except as referred to in section 69(1);
(g) not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his, her or its personal information intended to provide a profile of such person as provided for in terms of section 71;
(h) to submit a complaint to the Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a complaint to the Regulator in respect of a determination of an adjudicator as provided for in terms of section 74; and
(i) to institute civil proceedings regarding the alleged interference with the protection of his, her or its personal information as provided for in section 99.

Exclusions

6. (1) This Act does not apply to the processing of personal information—

(a) in the course of a purely personal or household activity;
(b) that has been de-identified to the extent that it cannot be re-identified again;
(c) by or on behalf of a public body—
  (i) which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defence or public safety; or

(ii) the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures,

to the extent that adequate safeguards have been established in legislation for the protection of such personal information;

(d) by the Cabinet and its committees or the Executive Council of a province; or

(e) relating to the judicial functions of a court referred to in section 166 of the Constitution.

(2) **"Terrorist and related activities"**, for purposes of subsection (1)*(c)*, means those activities referred to in section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004).

Exclusion for journalistic, literary or artistic purposes

7. (1) This Act does not apply to the processing of personal information solely for the purpose of journalistic, literary or artistic expression to the extent that such an exclusion is necessary to reconcile, as a matter of public interest, the right to privacy with the right to freedom of expression.

(2) Where a responsible party who processes personal information for exclusively journalistic purposes is, by virtue of office, employment or profession, subject to a code of ethics that provides adequate safeguards for the protection of personal information, such code will apply to the processing concerned to the exclusion of this Act and any alleged interference with the protection of the personal information of a data subject that may arise as a result of such processing must be adjudicated as provided for in terms of that code.

(3) In the event that a dispute may arise in respect of whether adequate safeguards have been provided for in a code as required in terms of subsection (2) or not, regard may be had to—

(a) the special importance of the public interest in freedom of expression;

(b) domestic and international standards balancing the—

(i) public interest in allowing for the free flow of information to the public through the media in recognition of the right of the public to be informed; and

(ii) public interest in safeguarding the protection of personal information of data subjects;

(c) the need to secure the integrity of personal information;

(d) domestic and international standards of professional integrity for journalists; and

(e) the nature and ambit of self-regulatory forms of supervision provided by the profession.

CHAPTER 3

CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

Part A

Processing of personal information in general

Condition 1

Accountability

Responsible party to ensure conditions for lawful processing

8. The responsible party must ensure that the conditions set out in this Chapter, and all the measures that give effect to such conditions, are complied with at the time of the

determination of the purpose and means of the processing and during the processing itself.

Condition 2

Processing limitation

Lawfulness of processing

9. Personal information must be processed—
(a) lawfully; and
(b) in a reasonable manner that does not infringe the privacy of the data subject.

Minimality

10. Personal information may only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive.

Consent, justification and objection

11. (1) Personal information may only be processed if—
(a) the data subject or a competent person where the data subject is a child consents to the processing;
(b) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;
(c) processing complies with an obligation imposed by law on the responsible party;
(d) processing protects a legitimate interest of the data subject;
(e) processing is necessary for the proper performance of a public law duty by a public body; or
(f) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

(2) *(a)* The responsible party bears the burden of proof for the data subject's or competent person's consent as referred to in subsection (1)*(a)*.

(b) The data subject or competent person may withdraw his, her or its consent, as referred to in subsection (1)*(a)*, at any time: Provided that the lawfulness of the processing of personal information before such withdrawal or the processing of personal information in terms of subsection (1)*(b)* to *(f)* will not be affected.

(3) A data subject may object, at any time, to the processing of personal information—
(a) in terms of subsection (1)*(d)* to *(f)*, in the prescribed manner, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or
(b) for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications as referred to in section 69.

(4) If a data subject has objected to the processing of personal information in terms of subsection (3), the responsible party may no longer process the personal information.

Collection directly from data subject

12. (1) Personal information must be collected directly from the data subject, except as otherwise provided for in subsection (2).

(2) It is not necessary to comply with subsection (1) if—
(a) the information is contained in or derived from a public record or has deliberately been made public by the data subject;
(b) the data subject or a competent person where the data subject is a child has consented to the collection of the information from another source;

(c) collection of the information from another source would not prejudice a legitimate interest of the data subject;
(d) collection of the information from another source is necessary—
(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;
(ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);
(iii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
(iv) in the interests of national security; or
(v) to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;
(e) compliance would prejudice a lawful purpose of the collection; or
(f) compliance is not reasonably practicable in the circumstances of the particular case.

Condition 3

Purpose specification

Collection for specific purpose

13. (1) Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

(2) Steps must be taken in accordance with section 18(1) to ensure that the data subject is aware of the purpose of the collection of the information unless the provisions of section 18(4) are applicable.

Retention and restriction of records

14. (1) Subject to subsections (2) and (3), records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless—
(a) retention of the record is required or authorised by law;
(b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities;
(c) retention of the record is required by a contract between the parties thereto; or
(d) the data subject or a competent person where the data subject is a child has consented to the retention of the record.

(2) Records of personal information may be retained for periods in excess of those contemplated in subsection (1) for historical, statistical or research purposes if the responsible party has established appropriate safeguards against the records being used for any other purposes.

(3) A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must—
(a) retain the record for such period as may be required or prescribed by law or a code of conduct; or
(b) if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

(4) A responsible party must destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after the responsible party is no longer authorised to retain the record in terms of subsection (1) or (2).

(5) The destruction or deletion of a record of personal information in terms of subsection (4) must be done in a manner that prevents its reconstruction in an intelligible form.

(6) The responsible party must restrict processing of personal information if—

(a) its accuracy is contested by the data subject, for a period enabling the responsible party to verify the accuracy of the information;

(b) the responsible party no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;

(c) the processing is unlawful and the data subject opposes its destruction or deletion and requests the restriction of its use instead; or

(d) the data subject requests to transmit the personal data into another automated processing system.

(7) Personal information referred to in subsection (6) may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or with the consent of a competent person in respect of a child, or for the protection of the rights of another natural or legal person or if such processing is in the public interest.

(8) Where processing of personal information is restricted pursuant to subsection (6), the responsible party must inform the data subject before lifting the restriction on processing.

Condition 4

Further processing limitation

Further processing to be compatible with purpose of collection

15. (1) Further processing of personal information must be in accordance or compatible with the purpose for which it was collected in terms of section 13.

(2) To assess whether further processing is compatible with the purpose of collection, the responsible party must take account of—

(a) the relationship between the purpose of the intended further processing and the purpose for which the information has been collected;

(b) the nature of the information concerned;

(c) the consequences of the intended further processing for the data subject;

(d) the manner in which the information has been collected; and

(e) any contractual rights and obligations between the parties.

(3) The further processing of personal information is not incompatible with the purpose of collection if—

(a) the data subject or a competent person where the data subject is a child has consented to the further processing of the information;

(b) the information is available in or derived from a public record or has deliberately been made public by the data subject;

(c) further processing is necessary—

(i) to avoid prejudice to the maintenance of the law by any public body including the prevention, detection, investigation, prosecution and punishment of offences;

(ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);

(iii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated; or

(iv) in the interests of national security;

(d) the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to—

(i) public health or public safety; or

(ii) the life or health of the data subject or another individual;

(e) the information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form; or

(f) the further processing of the information is in accordance with an exemption granted under section 37.

Condition 5

Information quality

Quality of information

16. (1) A responsible party must take reasonably practicable steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary.

(2) In taking the steps referred to in subsection (1), the responsible party must have regard to the purpose for which personal information is collected or further processed.

Condition 6

Openness

Documentation

17. A responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 14 or 51 of the Promotion of Access to Information Act.

Notification to data subject when collecting personal information

18. (1) If personal information is collected, the responsible party must take reasonably practicable steps to ensure that the data subject is aware of—

(a) the information being collected and where the information is not collected from the data subject, the source from which it is collected;

(b) the name and address of the responsible party;

(c) the purpose for which the information is being collected;

(d) whether or not the supply of the information by that data subject is voluntary or mandatory;

(e) the consequences of failure to provide the information;

(f) any particular law authorising or requiring the collection of the information;

(g) the fact that, where applicable, the responsible party intends to transfer the information to a third country or international organisation and the level of protection afforded to the information by that third country or international organisation;

(h) any further information such as the—

(i) recipient or category of recipients of the information;

(ii) nature or category of the information;

(iii) existence of the right of access to and the right to rectify the information collected;

(iv) existence of the right to object to the processing of personal information as referred to in section 11(3); and

(v) right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator,

which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

(2) The steps referred to in subsection (1) must be taken—

(a) if the personal information is collected directly from the data subject, before the information is collected, unless the data subject is already aware of the information referred to in that subsection; or

(b) in any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

(3) A responsible party that has previously taken the steps referred to in subsection (1) complies with subsection (1) in relation to the subsequent collection from the data subject of the same information or information of the same kind if the purpose of collection of the information remains the same.

(4) It is not necessary for a responsible party to comply with subsection (1) if—

(a) the data subject or a competent person where the data subject is a child has provided consent for the non-compliance;

(b) non-compliance would not prejudice the legitimate interests of the data subject as set out in terms of this Act;

(c) non-compliance is necessary—

(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

(ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);

(iii) for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or

(iv) in the interests of national security;

(d) compliance would prejudice a lawful purpose of the collection;

(e) compliance is not reasonably practicable in the circumstances of the particular case; or

(f) the information will—

(i) not be used in a form in which the data subject may be identified; or

(ii) be used for historical, statistical or research purposes.

Condition 7

Security Safeguards

Security measures on integrity and confidentiality of personal information

19. (1) A responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent—

(a) loss of, damage to or unauthorised destruction of personal information; and

(b) unlawful access to or processing of personal information.

(2) In order to give effect to subsection (1), the responsible party must take reasonable measures to—

(a) identify all reasonably foreseeable internal and external risks to personal information in its possession or under its control;

(b) establish and maintain appropriate safeguards against the risks identified;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

(3) The responsible party must have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

Information processed by operator or person acting under authority

20. An operator or anyone processing personal information on behalf of a responsible party or an operator, must—

(a) process such information only with the knowledge or authorisation of the responsible party; and

(b) treat personal information which comes to their knowledge as confidential and must not disclose it,

unless required by law or in the course of the proper performance of their duties.

Security measures regarding information processed by operator

21. (1) A responsible party must, in terms of a written contract between the responsible party and the operator, ensure that the operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 19.

(2) The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

Notification of security compromises

22. (1) Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify—

(a) the Regulator; and

(b) subject to subsection (3), the data subject, unless the identity of such data subject cannot be established.

(2) The notification referred to in subsection (1) must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

(3) The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

(4) The notification to a data subject referred to in subsection (1) must be in writing and communicated to the data subject in at least one of the following ways:

(a) Mailed to the data subject's last known physical or postal address;

(b) sent by e-mail to the data subject's last known e-mail address;

(c) placed in a prominent position on the website of the responsible party;

(d) published in the news media; or

(e) as may be directed by the Regulator.

(5) The notification referred to in subsection (1) must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including—

(a) a description of the possible consequences of the security compromise;

(b) a description of the measures that the responsible party intends to take or has taken to address the security compromise;

(c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and

(d) if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

(6) The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal

information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

Condition 8

Data subject participation

Access to personal information

23. (1) A data subject, having provided adequate proof of identity, has the right to—

(a) request a responsible party to confirm, free of charge, whether or not the responsible party holds personal information about the data subject; and

(b) request from a responsible party the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information—

(i) within a reasonable time;

(ii) at a prescribed fee, if any;

(iii) in a reasonable manner and format; and

(iv) in a form that is generally understandable.

(2) If, in response to a request in terms of subsection (1), personal information is communicated to a data subject, the data subject must be advised of the right in terms of section 24 to request the correction of information.

(3) If a data subject is required by a responsible party to pay a fee for services provided to the data subject in terms of subsection (1)*(b)* to enable the responsible party to respond to a request, the responsible party—

(a) must give the applicant a written estimate of the fee before providing the services; and

(b) may require the applicant to pay a deposit for all or part of the fee.

(4) *(a)* A responsible party may or must refuse, as the case may be, to disclose any information requested in terms of subsection (1) to which the grounds for refusal of access to records set out in the applicable sections of Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act apply.

(b) The provisions of sections 30 and 61 of the Promotion of Access to Information Act are applicable in respect of access to health or other records.

(5) If a request for access to personal information is made to a responsible party and part of that information may or must be refused in terms of subsection (4)*(a)*, every other part must be disclosed.

Correction of personal information

24. (1) A data subject may, in the prescribed manner, request a responsible party to—

(a) correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

(b) destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain in terms of section 14.

(2) On receipt of a request in terms of subsection (1) a responsible party must, as soon as reasonably practicable—

(a) correct the information;

(b) destroy or delete the information;

(c) provide the data subject, to his or her satisfaction, with credible evidence in support of the information; or