

“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; 5
- (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; 10
- (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; 15
- (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; 20

“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; 25
- (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— 30

- (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; 35

“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); 40

“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— 45
 - (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; 50

“record” means any recorded information—

- (a) regardless of form or medium, including any of the following: 55
 - (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; 60
 - (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 5
- (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; 10
- (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; 15

“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; 20

“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 25

“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 30

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 35
 - (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; 40
- (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. 45

CHAPTER 2

APPLICATION PROVISIONS

Application and interpretation of Act 50

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

- (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, 5
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. 10
- (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. 15

(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. 20 25

(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— 30
 - (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; 35
- (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. 40

CHAPTER 3

CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

Part A

Processing of personal information in general

Condition 1

45

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

5

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. 10

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; 15
- (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; 20
- (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). 25

(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. 30

(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. 35

(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). 40

(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; 45

- (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; 5
 - (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; 10
 - (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 15
- (f) compliance is not reasonably practicable in the circumstances of the particular case.

Condition 3

Purpose specification

Collection for specific purpose 20

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. 25

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; 30
- (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. 35

(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— 40

- (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. 45

(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). 50

(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; 5
- (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 10
- (d) the data subject requests to transmit the personal data into another automated processing system. 20

(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. 15

(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. 20

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. 25

(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; 30
- (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— 35

- (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— 40
 - (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); 45
 - (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— 50
 - (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. 5

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. 10

(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

15

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 20

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; 25
 - (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; 30
 - (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— 35
 - (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 40
 - (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. 45

(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 50

- (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. 5
- (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; 10
 - (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; 15
 - (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 20
 - (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— 25
 - (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 30

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. 35
- (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; 40
 - (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. 45

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

5

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.

10

15

(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—

20

- (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.

25

(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.

30

(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

35

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.

40

(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

45

- (d) where agreement cannot be reached between the responsible party and the data subject, and if the data subject so requests, take such steps as are reasonable in the circumstances, to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made. 5
- (3) If the responsible party has taken steps under subsection (2) that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the data subject in question, the responsible party must, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of those steps. 10
- (4) The responsible party must notify a data subject, who has made a request in terms of subsection (1), of the action taken as a result of the request.

Manner of access

25. The provisions of sections 18 and 53 of the Promotion of Access to Information Act apply to requests made in terms of section 23 of this Act. 15

Part B

Processing of special personal information

Prohibition on processing of special personal information

26. A responsible party may, subject to section 27, not process personal information concerning— 20
- (a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or
- (b) the criminal behaviour of a data subject to the extent that such information relates to— 25
- (i) the alleged commission by a data subject of any offence; or
- (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

General authorisation concerning special personal information

27. (1) The prohibition on processing personal information, as referred to in section 26, does not apply if the— 30
- (a) processing is carried out with the consent of a data subject referred to in section 26;
- (b) processing is necessary for the establishment, exercise or defence of a right or obligation in law; 35
- (c) processing is necessary to comply with an obligation of international public law;
- (d) processing is for historical, statistical or research purposes to the extent that— 40
- (i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or
- (ii) it appears to be impossible or would involve a disproportionate effort to ask for consent, 45
- and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent;
- (e) information has deliberately been made public by the data subject; or
- (f) provisions of sections 28 to 33 are, as the case may be, complied with.
- (2) The Regulator may, subject to subsection (3), upon application by a responsible party and by notice in the *Gazette*, authorise a responsible party to process special

- (b) about any further uses to which the directory may possibly be put, based on search functions embedded in electronic versions of the directory.
- (2) A data subject must be given a reasonable opportunity to object, free of charge and in a manner free of unnecessary formality, to such use of his, her or its personal information or to request verification, confirmation or withdrawal of such information if the data subject has not initially refused such use. 5
- (3) Subsections (1) and (2) do not apply to editions of directories that were produced in printed or off-line electronic form prior to the commencement of this section.
- (4) If the personal information of data subjects who are subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with the conditions for the lawful processing of personal information prior to the commencement of this section, the personal information of such subscribers may remain included in this public directory in its printed or electronic versions, after having received the information required by subsection (1). 10
- (5) “Subscriber”, for purposes of this section, means any person who is party to a contract with the provider of publicly available electronic communications services for the supply of such services. 15

Automated decision making

71. (1) Subject to subsection (2), a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct. 20
- (2) The provisions of subsection (1) do not apply if the decision— 25
- (a) has been taken in connection with the conclusion or execution of a contract, and—
- (i) the request of the data subject in terms of the contract has been met; or
- (ii) appropriate measures have been taken to protect the data subject’s legitimate interests; or 30
- (b) is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.
- (3) The appropriate measures, referred to in subsection (2)(a)(ii), must—
- (a) provide an opportunity for a data subject to make representations about a decision referred to in subsection (1); and 35
- (b) require a responsible party to provide a data subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make representations in terms of paragraph (a).

CHAPTER 9

40

TRANSBORDER INFORMATION FLOWS

Transfers of personal information outside Republic

72. (1) A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless—
- (a) the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that— 45
- (i) effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and 50

- (ii) includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;
- (b) the data subject consents to the transfer;
- (c) the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request; 5
- (d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or 10
- (e) the transfer is for the benefit of the data subject, and—
 - (i) it is not reasonably practicable to obtain the consent of the data subject to that transfer; and
 - (ii) if it were reasonably practicable to obtain such consent, the data subject would be likely to give it. 15
- (2) For the purpose of this section—
 - (a) **“binding corporate rules”** means personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country; and 20
 - (b) **“group of undertakings”** means a controlling undertaking and its controlled undertakings.

CHAPTER 10

ENFORCEMENT

25

Interference with protection of personal information of data subject

73. For the purposes of this Chapter, interference with the protection of the personal information of a data subject consists, in relation to that data subject, of—

- (a) any breach of the conditions for the lawful processing of personal information as referred to in Chapter 3; 30
- (b) non-compliance with section 22, 54, 69, 70, 71 or 72; or
- (c) a breach of the provisions of a code of conduct issued in terms of section 60.

Complaints

74. (1) Any person may submit a complaint to the Regulator in the prescribed manner and form alleging interference with the protection of the personal information of a data subject. 35

(2) A responsible party or data subject may, in terms of section 63(3), submit a complaint to the Regulator in the prescribed manner and form if he, she or it is aggrieved by the determination of an adjudicator.

Mode of complaints to Regulator

40

75. (1) A complaint to the Regulator must be made in writing.

(2) The Regulator must give such reasonable assistance as is necessary in the circumstances to enable a person, who wishes to make a complaint to the Regulator, to put the complaint in writing.

Action on receipt of complaint

45

76. (1) On receiving a complaint in terms of section 74, the Regulator may—

- (a) conduct a pre-investigation as referred to in section 79;