REPUBLIC OF SOUTH AFRICA

PROTECTION OF PERSONAL INFORMATION BILL

(As introduced in the National Assembly (proposed section 75); explanatory summary of Bill published in Government Gazette No. 32495 of 14 August 2009)
(The English text is the official text of the Bill)

(MINISTER OF JUSTICE AND CONSTITUTIONAL DEVELOPMENT)

[B 9—2009]

ISBN 978-1-77037-624-3

No. of copies printed 1 800

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.

BILL

To promote the protection of personal information processed by public and private bodies; to introduce information protection principles so as to establish minimum requirements for the processing of personal information; to provide for the establishment of an Information Protection Regulator; 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

CHAPTER 10

ENFORCEMENT

CHAPTER 11

OFFENCES AND PENALTIES

CHAPTER 12

GENERAL PROVISIONS

SCHEDULE

CHAPTER 1

DEFINITIONS AND PURPOSE

Definitions

1. In this Act, unless the context indicates otherwise—
"automatic calling machine" means a machine that is able to do automated calls without human intervention;

"biometric" means a technique of personal identification that is based on physical characteristics, including fingerprinting, DNA analysis, retinal scanning and voice recognition;

"child" means a natural person under the age of 18 years;

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

"consent" means any voluntary, specific and informed expression of will in terms of which a data subject agrees to the processing of personal information relating to him or her;

"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;

"electronic mail" or **"e-mail"** means any text, voice, sound or image message sent over a public communications network which can be 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 90;

"filing system" means any structured set of personal information which is accessible according to specific criteria;

"head" of, or in relation to, a private body means a head of a body as defined in section 1 of the Promotion of Access to Information Act;

"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 10 or more data subjects with one or more documents that contain personal information of 10 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 notice" means a notice issued in terms of section 88;

"information protection 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 of the Promotion of Access to Information Act; 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;

"parent" includes either the parent of a child or the child's legal guardian;

"parental consent" means any voluntary, specific and informed expression of will in terms of which the parent of a child agrees to the processing of personal information relating to that child;

"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 or other particular assignment to the person;

(d) the blood type or any other 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;

"prior investigation" means an investigation conducted by the Regulator in terms of Part B of Chapter 6;

"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 blocking, 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 communications network" means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services;

"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 Protection Regulator established in terms of section 35;

"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;

"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;

"subscriber" means any person who is party to a contract with the provider of publicly available electronic communications services for the supply of such services; and

"this Act" includes any regulation made under this Act.

Purpose of Act

2. (1) 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;
(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 principles, in harmony with international standards, that prescribe the minimum threshold requirements for 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 an Information Protection Regulator, to ensure respect for and to promote, enforce and fulfil the rights protected by this Act.

(2) This Act must be interpreted in a manner that—
(a) gives effect to the purposes of the Act set out in subsection (1); 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 functions, powers and duties relate to the processing of personal information and such processing is in accordance with this Act or any other legislation that regulates the processing of personal information.

CHAPTER 2

APPLICATION PROVISIONS

Application of Act

3. This Act applies to the processing of personal information entered in a record by or for a responsible party—
(a) domiciled in the Republic; or
(b) which is not domiciled in the Republic, using automated or non-automated means situated in the Republic, unless those means are used only for forwarding personal information,

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.

Exclusions

4. 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 the State and—
(i) which involves national security, defence or public safety; or

(ii) the purpose of which is the prevention, 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 specific legislation for the protection of such personal information;

(d) for exclusively journalistic purposes by responsible parties who are subject to, by virtue of office, employment or profession, a code of ethics that provides adequate safeguards for the protection of personal information;

(e) by Cabinet and its committees, the Executive Council of a province and a Municipal Council of a municipality;

(f) relating to the judicial functions of a court referred to in section 166 of the Constitution; or

(g) that has been exempted from the application of the information protection principles in terms of section 34.

Saving

5. (1) This Act does not affect the operation of any other legislation that regulates the processing of personal information and is capable of operating concurrently with this Act.

(2) If any other legislation provides for safeguards for the protection of personal information that are more extensive than those set out in the information protection principles, the extensive safeguards prevail.

Act applies to public and private bodies

6. This Act applies to all public and private bodies.

CHAPTER 3

CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

Part A

Information Protection Principles

Principle 1

Accountability

Responsible party to give effect to principles

7. The responsible party must ensure that the principles set out in this Chapter and all the measures that give effect to the principles are complied with.

Principle 2

Processing limitation

Lawfulness of processing

8. Personal information must be processed—

(a) lawfully; and

(b) in a reasonable manner that does not infringe the privacy of the data subject.

Minimality

9. 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

10. (1) Personal information may only be processed if—

(a) the data subject 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 data subject may object, at any time, on reasonable grounds relating to his, her or its particular situation, in the prescribed manner, to the processing of personal information in terms of subsection (1)*(d)* to *(f)*, unless otherwise provided for in national legislation.

(3) If a data subject has objected to the processing of personal information in terms of subsection (2), the responsible party may no longer process the personal information.

Collection directly from data subject

11. (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 a public record or has deliberately been made public by the data subject;
(b) the data subject 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 enforce a law imposing a pecuniary penalty;
(iii) 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);
(iv) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;
(v) in the legitimate interests of national security; or
(vi) 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.

Principle 3

Purpose specification

Collection for specific purpose

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

Data subject aware of purpose of collection of information

13. Steps must be taken in accordance with section 17(2) to ensure that the data subject is aware of the purpose of the collection of the information as referred to in section 12.

Retention 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 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.

Principle 4

Further processing limitation

Further processing to be compatible with purpose of collection

15. (1) Further processing of personal information must be compatible with the purpose for which it was collected in terms of principle 3.

(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 compatible with the purpose of collection if—

(a) the data subject has consented to the further processing of the information;

(b) the information is available in 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 enforce a law imposing a pecuniary penalty;

(iii) 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);

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

(v) in the legitimate 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 identified form; or

(f) the further processing of the information is in accordance with an authority granted under section 34.

Principle 5

Information quality

Quality of information

16. (1) The 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.

Principle 6

Openness

Notification to Regulator and to data subject

17. (1) Personal information may only be processed by a responsible party that has notified the Regulator in terms of Chapter 6.

(2) 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;

(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; and

(g) any further information, such as the—

(i) recipient or category of recipients of the information;
(ii) nature or category of the information; and
(iii) existence of the right of access to and the right to rectify the information collected,

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.

(3) The steps referred to in subsection (2) 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.

(4) A responsible party that compiles or has compiled a manual and made it available in terms of section 14 or 51 of the Promotion of Access to Information Act, does not have to comply with subsection (1) if all the particulars referred to in section 51 of this Act are contained in the manual.

(5) A responsible party that has previously taken the steps referred to in subsection (2) complies with subsection (2) 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 is unchanged.

(6) It is not necessary for a responsible party to comply with subsection (2) if—

(a) the data subject 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 enforce a law imposing a pecuniary penalty;
  (iii) 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);
  (iv) for the conduct of proceedings in any court or tribunal that have been commenced or are reasonably contemplated; or
  (v) 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.

Principle 7

Security Safeguards

Security measures on integrity of personal information

18. (1) A responsible party must secure the integrity 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

19. 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

20. (1) A responsible party must ensure that an operator which processes personal information for the responsible party establishes and maintains the security measures referred to in section 18.

(2) The processing of personal information for a responsible party by an operator on behalf of the responsible party must be governed by a written contract between the operator and the responsible party, which requires the operator to establish and maintain confidentiality and security measures to ensure the integrity of the personal information.

(3) If the operator is not domiciled in the Republic, the responsible party must take reasonably practicable steps to ensure that the operator complies with the laws, if any,

relating to the protection of personal information of the territory in which the operator is domiciled.

Notification of security compromises

21. (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, or any third party processing personal information under the authority of a responsible party, must notify the—

(a) Regulator; and

(b) 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 the South African Police Service, the National Intelligence Agency or the Regulator determines that notification will impede a criminal investigation.

(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) A notification must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including, 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.

Principle 8

Data subject participation

Access to personal information

22. (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 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, that is not excessive;

(iii) in a reasonable manner and format; and

(iv) in a form that is generally understandable.

(2) If, in accordance with subsection (1)*(b)*, personal information is communicated to a data subject, the data subject must be advised of the right in terms of section 23 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 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.

(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), every other part must be disclosed.

Correction of personal information

23. (1) A data subject may 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—

(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

(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.

(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.

(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

24. The provisions of sections 18 and 53 of the Promotion of Access to Information Act apply to requests made in terms of sections 22 and 23 of this Act.

Part B

Processing of special personal information

Prohibition on processing of special personal information

25. Unless specifically permitted by this Part, a responsible party may not process personal information concerning a—

(a) child who is subject to parental control in terms of the law; or

(b) data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life or criminal behaviour.

Exemption concerning data subject's religious or philosophical beliefs

26. (1) The prohibition on processing personal information concerning a data subject's religious or philosophical beliefs, as referred to in section 25, does not apply if the processing is carried out by—

(a) spiritual or religious organisations, or independent sections of those organisations: Provided that the information concerns data subjects belonging to those organisations;

(b) institutions founded on religious or philosophical principles with respect to their members or employees or other persons belonging to the institution, if it is necessary to achieve their aims and principles; or

(c) other institutions: Provided that the processing is necessary to protect the spiritual welfare of the data subjects, unless they have indicated that they object to the processing.

(2) In the cases referred to in subsection (1)*(a)*, the prohibition does not apply to processing of personal information concerning the religion or philosophy of life of family members of the data subjects, if—

(a) the association concerned maintains regular contact with those family members in connection with its aims; and

(b) the family members have not objected in writing to the processing.

(3) In the cases referred to in subsections (1) and (2), personal information concerning a data subject's religious or philosophical beliefs may not be supplied to third parties without the consent of the data subject.

Exemption concerning data subject's race

27. The prohibition on processing personal information concerning a data subject's race, as referred to in section 25, does not apply if the processing is carried out to—

(a) identify data subjects and only when this is essential for that purpose; and

(b) comply with laws and other measures designed to protect or advance persons, or categories of persons, disadvantaged by unfair discrimination.

Exemption concerning data subject's trade union membership

28. (1) The prohibition on processing personal information concerning a data subject's trade union membership, as referred to in section 25, does not apply to the processing by the trade union to which the data subject belongs or the trade union federation to which that trade union belongs, if such processing is necessary to achieve the aims of the trade union or trade union federation.

(2) In the cases referred to under subsection (1), no personal information may be supplied to third parties without the consent of the data subject.

Exemption concerning data subject's political persuasion

29. (1) The prohibition on processing personal information concerning a data subject's political persuasion, as referred to in section 25, does not apply to processing by an institution founded on political principles, of the personal information of their members or employees or other persons belonging to the institution, if such processing is necessary to achieve the aims or principles of the institutions.

(2) In the cases referred to under subsection (1), no personal information may be supplied to third parties without the consent of the data subject.

Exemption concerning data subject's health or sexual life

30. (1) The prohibition on processing personal information concerning a data subject's health or sexual life, as referred to in section 25, does not apply to the processing by—

(a) medical professionals, healthcare institutions or facilities or social services, if such processing is necessary for the proper treatment and care of the data subject, or for the administration of the institution or professional practice concerned;

(b) insurance companies, medical aid scheme administrators and managed healthcare organisations, if such processing is necessary for—

(i) assessing the risk to be insured by the insurance company or covered by the medical aid scheme and the data subject has not objected to the processing;

(ii) the performance of an insurance or medical aid agreement; or

(iii) the enforcement of any contractual rights and obligations;

(c) schools, if such processing is necessary to provide special support for pupils or making special arrangements in connection with their health or sexual life;

(d) institutions of probation, child protection or guardianship, if such processing is necessary for the performance of their legal duties;

(e) the Minister and the Minister of Correctional Services, if such processing is necessary in connection with the implementation of prison sentences or detention measures; or

(f) administrative bodies, pension funds, employers or institutions working for them, if such processing is necessary for—

(i) the implementation of the provisions of laws, pension regulations or collective agreements which create rights dependent on the health or sexual life of the data subject; or

(ii) the reintegration of or support for workers or persons entitled to benefit in connection with sickness or work incapacity.

(2) In the cases referred to under subsection (1), the information may only be processed by responsible parties subject to an obligation of confidentiality by virtue of office, employment, profession or legal provision, or established by a written agreement between the responsible party and the data subject.

(3) A responsible party that is permitted to process information concerning a data subject's health or sexual life in terms of this section and is not subject to an obligation of confidentiality by virtue of office, profession or legal provision, must treat the information as confidential, unless the responsible party is required by law or in connection with their duties to communicate the information to other parties who are authorised to process such information in accordance with subsection (1).

(4) The prohibition on processing any of the categories of personal information referred to in section 25, does not apply if it is necessary to supplement the processing of personal information concerning a data subject's health, as referred to under subsection (1)*(a)*, with a view to the proper treatment or care of the data subject.

(5) Personal information concerning inherited characteristics may not be processed in respect of a data subject from whom the information concerned has been obtained, unless—

(a) a serious medical interest prevails; or

(b) the processing is necessary for the purpose of scientific research or statistics.

(6) More detailed rules may be prescribed concerning the application of subsection (1)*(b)* and *(f)*.

Exemption concerning data subject's criminal behaviour

31. (1) The prohibition on processing personal information concerning a data subject's criminal behaviour, as referred to in section 25, does not apply if the processing is carried out by bodies charged by law with applying criminal law or by responsible parties who have obtained that information in accordance with the law.

(2) The prohibition does not apply to responsible parties who process the information for their own lawful purposes to—

(a) assess an application by a data subject in order to take a decision about, or provide a service to, that data subject; or

(b) protect their legitimate interests in relation to criminal offences which have been, or can reasonably be expected to be, committed against them or against persons in their service.

(3) The processing of information concerning personnel in the service of the responsible party must take place in accordance with the rules established in compliance with labour legislation.

(4) The prohibition on processing any of the categories of personnel information referred to in section 26 does not apply if such processing is necessary to supplement the processing of information on criminal behaviour permitted by this section.

General exemption concerning special personal information

32. Without prejudice to sections 26 to 31, the prohibition on processing personal information, as referred to in section 25, does not apply if—

(a) processing is carried out with prior parental consent where the data subject is a child and is subject to parental control in terms of the law;

(b) processing is necessary for the establishment, exercise or defence of a right or obligation in law;

(c) processing is necessary to comply with an obligation of international public law;

(d) the Regulator has granted authority in terms of section 34 for processing in the public interest, and appropriate guarantees have been put in place in law to protect the data subject's privacy; or

(e) insofar as section 25*(b)* is concerned—

(i) processing is carried out with the consent of the data subject; or

(ii) the information has deliberately been made public by the data subject.

CHAPTER 4

EXEMPTION FROM INFORMATION PROTECTION PRINCIPLES

General

33. Processing of personal information is not in breach of an information protection principle if the processing is authorised by the Regulator in terms of section 34.

Regulator may authorise processing of personal information

34. (1) The Regulator may authorise a responsible party to process personal information, even if that processing is in breach of an information protection principle if the Regulator is satisfied that, in the circumstances of the case—

(a) the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from such processing; or

(b) the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from such processing.

(2) The public interest referred to in subsection (1) includes—

(a) the legitimate interests of State security;

(b) the prevention, detection and prosecution of offences;

(c) important economic and financial interests of the State or a public body;

(d) fostering compliance with legal provisions established in the interests referred to under paragraphs *(b)* and *(c)*; or

(e) historical, statistical or research activity.

(3) The Regulator may impose reasonable conditions in respect of any authorisation granted under subsection (1).

CHAPTER 5

SUPERVISION

Part A

Information Protection Regulator

Establishment of Information Protection Regulator

35. There is hereby established a juristic person to be known as the Information Protection Regulator, which—

(a) has jurisdiction throughout the Republic;

(b) is independent and is subject only to the Constitution and to the law and must be impartial and perform its functions and exercise its powers without fear, favour or prejudice; and

(c) must perform its functions and exercise its powers in accordance with this Act and the Promotion of Access to Information Act.

Constitution and term of office of Regulator

36. (1) *(a)* The Regulator consists of the following members:

(i) A Chairperson; and

(ii) four other persons, as ordinary members of the Regulator.

(b) Members of the Regulator must be appropriately qualified, fit and proper persons for appointment on account of experience as a practicing advocate or attorney or a

professor of law at a university, or on account of any other qualification relating to the objects of the Regulator.

(c) The Chairperson of the Regulator must perform his or her functions under the Act and the Promotion of Access to Information Act in a full-time capacity and must not be employed in any other capacity during the period in which he or she holds office as Chairperson.

(d) The other members of the Regulator must be appointed in a part-time capacity.

(e) The Chairperson must direct the work of the Regulator and the Secretariat.

(f) No person will be qualified for appointment as a member of the Regulator if that person—

(i) is a member of a legislature;

(ii) is a councillor of a local authority;

(iii) is an unrehabilitated insolvent; or

(iv) has at any time been convicted of any offence involving dishonesty.

(2) Members of the Regulator referred to in subsection (1)*(a)* must be appointed by the President and must be persons approved by Parliament, after considering proposals made by interested parties in terms of subsection (4).

(3) The President may appoint one or more additional members if he or she considers it necessary for the investigation of any particular matter or the performance of any duty by the Regulator.

(4) Before the members of the Regulator are appointed the Minister must invite interested parties through the media and by notice in the *Gazette* to propose candidates within 30 days of the publication of such notice, for consideration as contemplated in subsection (2).

(5) The members of the Regulator will be appointed for a period of not more than five years and will, at the expiration of such period, be eligible for reappointment.

(6) A person appointed as a member of the Regulator may resign from office by writing under his or her hand addressed to the President and will in any case vacate office on attaining the age of 70 years.

(7) A member may be removed from office by the President on the request of Parliament only for inability to discharge the functions of the office, whether arising from infirmity of body or mind or any other cause, or for misbehaviour.

Remuneration, allowances, benefits and privileges of members

37. (1) A member of the Regulator who is not subject to the provisions of the Public Service Act, 1994 (Proclamation No. 103 of 1994), will be entitled to such remuneration, allowances, including allowances for reimbursement of travelling and subsistence expenses incurred by him or her in the performance of his or her functions under this Act and the Promotion of Access to Information Act, benefits and privileges as the Minister in consultation with the Minister of Finance may determine.

(2) The remuneration, allowances, benefits or privileges of different members of the Regulator may differ according to the different —

(a) offices held by them in the Regulator; or

(b) functions performed, whether in a part-time or full-time capacity, by them from time to time.

(3) In the application of subsections (1) and (2), the President or the Minister, as the case may be, may determine that any remuneration, allowance, benefit or privilege contemplated in those subsections will be the remuneration, allowance, benefit or privilege determined from time to time by or under any law in respect of any person or category of persons.

Secretary and staff

38. (1) The Secretary of the Regulator and such other officers and employees as are required for the proper performance of the Regulator's functions, will be appointed in terms of the Public Service Act, 1994 (Proclamation No. 103 of 1994).

(2) The Regulator may, with the approval of the Minister in consultation with the Minister of Finance, on a temporary basis or for a particular matter which is being investigated by it, employ any person with special knowledge of any matter relating to the work of the Regulator, or obtain the co-operation of any body, to advise or assist the Regulator in the performance of its functions under this Act and the Promotion of Access to Information Act, and fix the remuneration, including reimbursement for travelling, subsistence and other expenses, of such person or body.

Committees of Regulator

39. (1) The Regulator may, if it considers it necessary for the proper performance of its functions, establish—

(a) a working committee, which must consist of such members of the Regulator as the Regulator may designate;

(b) such other committees as it may deem necessary, and which must consist of—

(i) such members of the Regulator as the Regulator may designate; or

(ii) such members of the Regulator as the Regulator may designate and other persons appointed by the Minister for the period determined by the Minister.

(2) The Minister may at any time extend the period of an appointment referred to in subsection (1)*(b)*(ii) or, if in his or her opinion good reasons exist therefor, revoke any such appointment.

(3) The Regulator must designate the chairperson and, if the Regulator deems it necessary, the vice-chairperson of a committee established under subsection (1).

(4) *(a)* A committee referred to in subsection (1) must, subject to the directions of the Regulator, perform those functions of the Regulator assigned to it by the Regulator.

(b) Any function so performed by the working committee referred to in subsection (1)*(a)* will be deemed to have been performed by the Regulator.

(5) The Regulator may at any time dissolve any committee established by the Regulator.

(6) The provisions of sections 40 and 45(4) will apply, with the necessary changes, to a committee of the Regulator.

Meetings of Regulator

40. (1) Meetings of the Regulator must be held at the times and places determined by the Chairperson of the Regulator.

(2) The majority of the members of the Regulator will constitute a quorum for a meeting.

(3) The Regulator may regulate the proceedings at meetings as it may think fit and must keep minutes of the proceedings.

Funds

41. (1) Parliament must appropriate annually, for the use of the Regulator, such sums of money as may be necessary for the proper exercise, performance and discharge, by the Regulator, of its powers, duties and functions under this Act and the Promotion of Access to Information Act.

(2) The financial year of the Regulator is the period from 1 April in any year to 31 March in the following year, except that the first financial year of the Regulator begins on the date that this Act comes into operation, and ends on 31 March next following that date.

(3) The Chairperson of the Regulator is the accounting authority of the Regulator for purposes of the Public Finance Management Act, 1999 (Act No. 1 of 1999), and must execute his or her duties in accordance with that Act.

(4) Within six months after the end of each financial year, the Regulator must prepare financial statements in accordance with established accounting practice, principles and procedures, comprising—

(a) a statement reflecting, with suitable and sufficient particulars, the income and expenditure of the Regulator during the preceding financial year; and

(b) a balance sheet showing the state of its assets, liabilities and financial position as at the end of that financial year.

(5) The Auditor-General must audit the Regulator's financial records each year.

Protection of Regulator

42. The Regulator, or any person acting on behalf or under the direction of the Regulator, is not civilly or criminally liable for anything done in good faith in the exercise or performance or purported exercise or performance of any power, duty or function of the Regulator in terms of this Act or the Promotion of Access to Information Act.

Powers and duties of Regulator

43. (1) The powers and duties of the Regulator in terms of this Act are—

(a) to promote, by education and publicity, an understanding and acceptance of the information protection principles and of the objects of those principles;

(b) for the purpose of promoting the protection of personal information, to undertake educational programmes on the Regulator's own behalf or in co-operation with other persons or authorities acting on behalf of the Regulator;

(c) to make public statements in relation to any matter affecting the protection of the personal information of a data subject or of any class of data subjects;

(d) to monitor and enforce compliance by public and private bodies of the provisions of this Act;

(e) to undertake research into, and to monitor developments in, information processing and computer technology to ensure that any adverse effects of such developments on the protection of the personal information of data subjects are minimised, and to report to the Minister the results of such research and monitoring;

(f) to examine any proposed legislation, including subordinate legislation, or proposed policy of the Government that the Regulator considers may affect the protection of the personal information of data subjects, and to report to the Minister the results of that examination;

(g) to report, with or without request, to Parliament from time to time on any matter affecting the protection of the personal information of a data subject, including the need for, or desirability of, taking legislative, administrative or other action to give protection or better protection to the personal information of a data subject;

(h) when requested to do so by a public or private body, to conduct an audit of personal information maintained by that body for the purpose of ascertaining whether or not the information is maintained according to the information protection principles;

(i) to monitor the use of unique identifiers of data subjects, and to report to Parliament from time to time on the results of that monitoring, including any recommendation relating to the need of, or desirability of taking, legislative, administrative or other action to give protection, or better protection, to the personal information of a data subject;

(j) to maintain, and to publish, make available and provide copies of such registers as are prescribed in terms of this Act;

(k) to examine any proposed legislation that makes provision for the—

(i) collection of personal information by any public or private body; or

(ii) disclosure of personal information by one public or private body to any other public or private body, or both, to have particular regard, in the course of that examination, to the matters set out in section 44(3) of this Act, in any case where the Regulator considers that the information might be used for the purposes of an information matching programme,

and to report to the Minister and Parliament the results of that examination;

(l) to receive and invite representations from members of the public on any matter affecting the personal information of a data subject;

(m) to consult and co-operate with other persons and bodies concerned with the protection of personal information principles;

(n) to act as mediator between opposing parties on any matter that concerns the need for, or the desirability of, action by a responsible party in the interests of the protection of the personal information of a data subject;

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

(p) to receive and investigate complaints about alleged violations of the protection of personal information of data subjects and in respect thereof make reports to complainants;

(q) to gather such information as in the Regulator's opinion will assist the Regulator in discharging the duties and carrying out the Regulator's functions under this Act;

(r) to attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation;

(s) to serve any notices in terms of this Act and further promote the resolution of disputes in accordance with the prescripts of this Act;

(t) to report to Parliament from time to time on the desirability of the acceptance, by South Africa, of any international instrument relating to the protection of the personal information of a data subject;

(u) to report to Parliament on any other matter relating to protection of personal information that, in the Regulator's opinion, should be drawn to Parliament's attention;

(v) to issue, from time to time, codes of conduct, amendment of codes and revocation of codes of conduct;

(w) to make guidelines to assist bodies to develop codes of conduct or to apply codes of conduct;

(x) to review an adjudicator's decision under approved codes of conduct;

(y) to do anything incidental or conducive to the performance of any of the preceding functions;

(z) to exercise and perform such other functions, powers and duties as are conferred or imposed on the Regulator by or under this Act or any other enactment;

(aa) to require the responsible party to disclose to any person affected by a compromise to the confidentiality or integrity of personal information, this fact in accordance with section 21 of this Act; and

(bb) to exercise the powers conferred upon the Regulator by this Act in matters relating to the access of information as provided by the Promotion of Access to Information Act.

(2) The Regulator may, from time to time, in the public interest or in the legitimate interests of any person or body of persons, publish reports relating generally to the exercise of the Regulator's functions under this Act or to any case or cases investigated by the Regulator, whether or not the matters to be dealt with in any such report have been the subject of a report to the Minister.

(3) The powers and duties of the Regulator in terms of the Promotion of Access to Information Act are set out in Part 5 of that Act.

Regulator to have regard to certain matters

44. (1) The Regulator is independent in the performance of its functions as set out in section 35*(b)*.

(2) In the performance of its functions and the exercise of its powers under this Act, the Regulator must—

(a) have due regard to the protection of personal information as set out in the information protection principles;

(b) have due regard for the protection of all human rights and social interests that compete with privacy, including the general desirability of a free flow of information and the recognition of the legitimate interests of government and business in achieving their objectives in an efficient way;

(c) take account of international obligations accepted by South Africa, including those concerning the international technology of communications; and

(d) consider any developing general international guidelines relevant to the better protection of individual privacy.

(3) In performing its functions in terms of section 43(1)*(k)* with regard to information matching programmes, the Regulator must have particular regard to whether or not the—

(a) objective of the programme relates to a matter of significant public importance;

(b) use of the programme to achieve that objective will result in monetary savings that are both significant and quantifiable or in other comparable benefits to society;

(c) use of an alternative means of achieving that objective would give either of the results referred to in paragraph *(b)*;

(d) public interest in allowing the programme to proceed outweighs the public interest in adhering to the information protection principles that the programme would otherwise contravene; and

(e) programme involves information matching on a scale that is excessive, having regard to—

(i) the number of responsible parties or operators that will be involved in the programme; and

(ii) the amount of detail about a data subject that will be matched under the programme.

Programmes of Regulator

45. (1) In order to achieve its objects in terms of this Act the Regulator must from time to time draw up programmes in which the various matters which in its opinion require consideration are included in order of preference, and must table such programmes in Parliament for information.

(2) The Regulator may include in any programme any suggestion relating to its objects received from any person or body.

(3) The Regulator may consult any person or body, whether by the submission of study documents prepared by the Regulator or in any other manner.

(4) The provisions of sections 2, 3, 4, 5 and 6 of the Commission's Act, 1947 (Act No. 8 of 1947), will apply, with the necessary changes, to the Regulator.

Reports of Regulator

46. (1) The Regulator must prepare a full report in regard to any matter investigated by it in terms of this Act and must submit such report to Parliament for information.

(2) The Regulator must within five months of the end of a financial year of the Department of Justice and Constitutional Development submit to the Minister a report on all its activities in terms of this Act during that financial year.

(3) The report referred to in subsection (2) must be tabled in Parliament within 14 days after it was submitted to the Minister, if Parliament is then in session, or, if Parliament is not in session, within 14 days after the commencement of its next ensuing session.

Duty of confidentiality

47. A person acting on behalf or under the direction of the Regulator, must treat as confidential the personal information which comes to his or her knowledge, except if the communication of such information is required by law or in the proper performance of his or her duties.

Part B

Information Protection Officer

Duties and responsibilities of Information Protection Officer

48. (1) An information protection officer's responsibilities include—

(a) the encouragement of compliance, by the body, with the information protection principles;

(b) dealing with requests made to the body pursuant to this Act;

(c) working with the Regulator in relation to investigations conducted pursuant to Chapter 6 in relation to the body; and

(d) otherwise ensuring compliance by the body with the provisions of this Act.

(2) Officers must take up their duties in terms of this Act only after the responsible party has registered them with the Regulator.

Designation and delegation of deputy information protection officers

49. Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of—

(a) such a number of persons, if any, as deputy information protection officers as is necessary to perform the duties and responsibilities as set out in section 48(1) of this Act; and

(b) any power or duty conferred or imposed on an information protection officer by this Act to a deputy information protection officer of that public or private body.

CHAPTER 6

NOTIFICATION AND PRIOR INVESTIGATION

Part A

Notification

Notification of processing

50. (1) A responsible party must notify the Regulator before commencing the—

(a) fully or partly automated processing of personal information or categories of personal information intended to serve a single purpose or different related purposes; and

(b) non-automated processing of personal information intended to serve a single purpose or different related purposes, must be notified if this is subject to a prior investigation.

(2) The notification referred to in subsection (1) must be noted in a register kept by the Regulator for this purpose.

Notification to contain specific particulars

51. (1) The notification must contain the following particulars:

(a) The name and address of the responsible party;

(b) the purpose of the processing;

(c) a description of the categories of data subjects and of the information or categories of information relating thereto;

(d) the recipients or categories of recipients to whom the personal information may be supplied;

(e) planned transborder flows of personal information; and

(f) a general description allowing a preliminary assessment of the suitability of the information security measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information which is to be processed.

(2) Subject to subsection (3) a responsible party will only have to give notice once, and not each time personal information is received or processed.

(3) Changes in the name or address of the responsible party must be notified within one week and changes to the notification which concern subsection (1)*(b)* to *(f)* must be notified in each case within one year of the previous notification, if they are of more than incidental importance.

(4) Any processing which departs from that which has been notified in accordance with the provisions of subsection (1)*(b)* to *(f)* must be recorded and kept for at least three years.

(5) More detailed rules may be prescribed concerning the procedure for submitting notifications.

Exemptions to notification requirements

52. (1) The Regulator may by notice exempt certain categories of information processing which are unlikely to infringe the legitimate interests of a data subject from the notification requirement referred to in section 50.

(2) If processing of personal information is necessary in order to detect offences in a particular case, it may be prescribed that certain categories of processing by responsible parties who are vested with investigating powers by law, are exempt from notification.

(3) The notification requirement does not apply to public registers set up by law or to information supplied to a public body pursuant to a legal obligation.

(4) Any exemption granted to a responsible party from the provisions set out in section 14 or 51 of the Promotion of Access to Information Act will also apply as an exemption of the notification requirements set out in terms of this Act.

Register of information processing

53. (1) The Regulator must maintain an up-to-date register of the information processing notified to it, which register must contain, as a minimum, the information provided in accordance with section 51(1).

(2) The register may be consulted by any person free of charge.

(3) The responsible party must provide any person who requests information referred to in section 50(1) with the information so requested.

(4) The provisions of subsection (3) do not apply to—

(a) information processing which is covered by an exemption under Chapter 4; and

(b) public registers set up by law.

Failure to notify

54. (1) If section 50(1) is contravened, the responsible party is guilty of an offence and liable to a penalty as set out in section 99.

(2) Any responsible party who fails to comply with the duty imposed by notification regulations made by virtue of section 102 is guilty of an offence and liable to a penalty as set out in section 99.

Part B

Prior investigation

Processing subject to prior investigation

55. (1) The Regulator must initiate an investigation prior to any processing if a responsible party plans to—

(a) process a number identifying data subjects for a purpose other than the one for which the number is specifically intended with the aim of linking the information together with information processed by other responsible parties, unless the number is used for the cases defined in Chapter 4;

(b) process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;

(c) process information for the purposes of credit reporting; and

(d) transfer special personal information, as referred to in section 26, to foreign countries without adequate information protection laws.

(2) The provisions of subsection (1) may be applied by the Regulator to other types of information processing by law or regulation if such processing carries a particular risk for the legitimate interests of the data subject.

(3) Part B of Chapter 6 will not be applicable if a code of conduct has been issued and has come into force in terms of Chapter 7 in a specific sector or sectors of society.

Responsible party to notify Regulator if processing is subject to prior investigation

56. (1) Information processing under a code of conduct as contemplated in section 55(3) must be notified as such by the responsible party to the Regulator.

(2) Responsible parties may not carry out information processing that has been notified to the Regulator in terms of subsection (1) until the Regulator has completed its investigation or until they have received notice that a more detailed investigation will not be conducted.

(3) In the case of the notification of information processing to which section 55(1) is applicable, the Regulator must inform the responsible party in writing within four weeks of the notification as to whether or not it will conduct a more detailed investigation.

(4) In the event that the Regulator decides to conduct a more detailed investigation, it must indicate the period within which it plans to conduct this investigation, which period must not exceed 13 weeks.

(5) On conclusion of the more detailed investigation referred to in subsection (4) the Regulator must issue a statement concerning the lawfulness of the information processing.

(6) A statement by the Regulator in terms of subsection (5) is deemed to be an enforcement notice served in terms of section 90 of this Act.

(7) A responsible party that has suspended its processing as required by subsection (2), and which has not received the Regulator's decision within the time limits specified in subsections (3) and (4), may presume a decision in its favour and continue with its processing.

CHAPTER 7

CODES OF CONDUCT

Issuing of codes of conduct

57. (1) The Regulator may from time to time issue a code of conduct.

(2) A code of conduct must—

(a) incorporate all the information protection principles or set out obligations that provide a functional equivalent of all the obligations set out in those principles; and

(b) prescribe how the information protection principles are to be applied, or are to be complied with, given the particular features of the sector or sectors of society in which the relevant responsible parties are operating.

(3) A code of conduct may apply in relation to any one or more of the following:

(a) Any specified information or class of information;

(b) any specified body or class of bodies;

(c) any specified activity or class of activities;

(d) any specified industry, profession, or calling or class of industries, professions or callings.

(4) A code of conduct must also—

(a) in relation to any body that is not a public body, provide for controls in relation to the comparison, whether manually or by means of any electronic or other device, of personal information with other personal information for the purpose of producing or verifying information about an identifiable data subject;

(b) provide for the review of the code by the Regulator; and

(c) provide for the expiry of the code.

Proposal for issuing of code of conduct

58. (1) The Regulator may issue a code of conduct under section 57 of this Act—

(a) on the Regulator's own initiative but in consultation with affected stakeholders or a body representing such stakeholders; or

(b) on the application of any person as provided in subsection (3).

(2) Without limiting subsection (1), but subject to subsection (3), any person may apply to the Regulator for the issuing of a code of conduct in the prescribed form submitted by the applicant.

(3) An application may be made pursuant to subsection (2) only—

(a) by a body which is, in the opinion of the Regulator, sufficiently representative of any class of bodies, or of any industry, profession or calling as defined in the code; and

(b) if the code of conduct sought by the applicant is intended to apply in respect of the class of body, or the industry, profession or calling, that the applicant represents,

in respect of such class of body or of any such industry, profession or calling.

(4) If an application is made to the Regulator pursuant to subsection (2), or if the Regulator intends to issue a code on its own initiative, the Regulator must give notice in the *Gazette* that the issuing of a code of conduct is being considered, which notice must contain a statement that—

(a) the details of the code of conduct being considered, including a draft of the proposed code, may be obtained from the Regulator; and

(b) submissions on the proposed code may be made in writing to the Regulator within such period as is specified in the notice.

(5) The Regulator must not issue a code of conduct unless it has considered the submissions made to the Regulator in terms of subsection (4), if any, and is satisfied that all persons affected by the proposed code have had a reasonable opportunity to be heard.

(6) The decision as to whether an application for the issuing of a code has been successful must be made within a reasonable period which must not exceed 13 weeks.

Notification, availability and commencement of code

59. (1) If a code of conduct is issued under section 57—

(a) the Regulator must ensure that there is published in the *Gazette*, as soon as reasonably practicable after the code is issued, a notice indicating—

(i) that the code has been issued; and

(ii) where copies of the code are available for inspection free of charge and for purchase; and

(b) the Regulator must ensure that as long as the code remains in force, copies of it are available—

(i) on the Regulator's website;

(ii) for inspection by members of the public free of charge at the Regulator's offices; and

(iii) for purchase or copying by members of the public at a reasonable price at the Regulator's offices.

(2) A code of conduct issued under section 57 comes into force on the 28th day after the date of its notification in the *Gazette* or on such later date as may be specified in the code and is binding on every class or classes of body, industry, profession or calling referred to therein.

Amendment and revocation of codes

60. (1) The Regulator may amend or revoke a code of conduct issued under section 57.

(2) The provisions of sections 57, 58, 59 and 61 apply in respect of any amendment or revocation of a code of conduct.

Procedure for dealing with complaints

61. (1) A code of conduct may prescribe procedures for making and dealing with complaints alleging a breach of the code, but no such provision may limit or restrict any provision of Chapter 8.

(2) If the code sets out procedures for making and dealing with complaints, the Regulator must be satisfied that—

(a) the procedures meet the—

(i) prescribed standards; and

(ii) guidelines issued by the Regulator in terms of section 62,

relating to the making of and dealing with complaints;

(b) the code provides for the appointment of an independent adjudicator to whom complaints may be made;

(c) the code provides that, in performing his or her functions and exercising his or her powers under the code, an adjudicator for the code must have due regard to the matters listed in section 44(2);

(d) the code requires the adjudicator to prepare and submit a report, in a form satisfactory to the Regulator, to the Regulator within five months of the end of

a financial year of the Department of Justice and Constitutional Development on the operation of the code during that financial year; and

(e) the code requires the report prepared for each year to specify the number and nature of complaints made to an adjudicator under the code during the relevant financial year.

(3) A data subject who is aggrieved by a determination, including any declaration, order or direction that is included in the determination made by an adjudicator, other than the Regulator, after investigating a complaint relating to the protection of personal information under an approved code of conduct, may lodge a complaint with the Regulator against the determination on payment of a prescribed fee.

(4) The adjudicator's determination continues to have effect unless and until the Regulator makes a determination under Chapter 10 relating to the complaint.

Guidelines about codes of conduct

62. (1) The Regulator may provide written guidelines—

(a) to assist bodies to develop codes of conduct or to apply approved codes of conduct;

(b) relating to making and dealing with complaints under approved codes of conduct; and

(c) about matters the Regulator may consider in deciding whether to approve a code of conduct or a variation of an approved code of conduct.

(2) Before providing guidelines for the purposes of subsection (1)*(b)*, the Regulator must give everyone the Regulator considers has a real and substantial legitimate interest in the matters covered by the proposed guidelines an opportunity to comment on them.

(3) The Regulator must publish guidelines provided under subsection (1) in the *Gazette*.

Register of approved codes of conduct

63. (1) The Regulator must keep a register of approved codes of conduct.

(2) The Regulator may decide the form of the register and how it is to be kept.

(3) The Regulator must make the register available to the public in the way that the Regulator determines.

(4) The Regulator may charge reasonable fees for—

(a) making the register available to the public; or

(b) providing copies of, or extracts from, the register.

Review of operation of approved code of conduct

64. (1) The Regulator may, on its own initiative, review the operation of an approved code of conduct.

(2) The Regulator may do one or more of the following for the purposes of the review:

(a) Consider the process under the code for making and dealing with complaints;

(b) inspect the records of an adjudicator for the code;

(c) consider the outcome of complaints dealt with under the code;

(d) interview an adjudicator for the code; and

(e) appoint experts to review those provisions of the code that the Regulator believes require expert evaluation.

(3) The review may inform a decision by the Regulator under section 60 to revoke the approved code of conduct with immediate effect or at a future date to be determined by the Regulator.

Effect of failure to comply with code

65. If a code issued under section 57 of this Act is in force, failure to comply with the code is deemed to be a breach of an information protection principle.

CHAPTER 8

RIGHTS OF DATA SUBJECTS REGARDING UNSOLICITED ELECTRONIC COMMUNICATIONS AND AUTOMATED DECISION MAKING

Unsolicited electronic communications

66. (1) The processing of personal information of a data subject for the purpose of direct marketing by means of automatic calling machines, facsimile machines, SMSs or electronic mail is prohibited unless the data subject—

(a) has given his, her or its consent to the processing; or

(b) is, subject to subsection (2), a customer of the responsible party.

(2) A responsible party may only process the personal information of a data subject who is a customer of the responsible party in terms of subsection (1)*(b)*—

(a) if the responsible party has obtained the contact details of the data subject in the context of the sale of a product or service;

(b) for the purpose of direct marketing of the responsible party's own similar products or services; and

(c) if the data subject has been 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 electronic details—

(i) at the time when the information was collected; and

(ii) on the occasion of each communication with the data subject for the purpose of marketing if the data subject has not initially refused such use.

(3) Any communication for the purpose of direct marketing must contain—

(a) details of the identity of the sender or the person on whose behalf the communication has been sent; and

(b) an address or other contact details to which the recipient may send a request that such communications cease.

Directories

67. (1) A data subject who is a subscriber to a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which his, her or its personal information is included, must be informed, free of charge and before the information is included in the directory—

(a) about the purpose of the directory; and

(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.

(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 information protection principles 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).

Automated decision making

68. (1) Subject to subsection (2), no one may be subject to a decision to which are attached legal consequences for him or her, or which affects him or her to a substantial degree, that has been taken solely on the basis of the automated processing of personal information intended to provide a profile of certain aspects of his or her personality or personal habits.

(2) The provisions of subsection (1) do not apply if the decision—

(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

(b) is governed by a law or code 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

(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

TRANSBORDER INFORMATION FLOWS

Transfers of personal information outside Republic

69. 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 recipient of the information is subject to a law, binding code of conduct or contract which—

(i) effectively upholds principles for reasonable processing of the information that are substantially similar to the information protection principles; and

(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;

(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

(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.

CHAPTER 10

ENFORCEMENT

Interference with protection of personal information of data subject

70. 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 information protection principles set out in Chapter 3;

(b) non-compliance with section 21, 47, 66, 67, 68 or 69; or

(c) a breach of the provisions of a code of conduct issued in terms of section 57.

Complaints

71. Any person may submit a complaint to the Regulator in the prescribed manner and form—

(a) alleging interference with the protection of the personal information of a data subject; or

(b) in terms of section 61(3) if the data subject is aggrieved by the determination of an adjudicator.

Mode of complaints to Regulator

72. (1) A complaint to the Regulator may be made either orally or in writing.

(2) A complaint made orally must be put in writing as soon as reasonably practicable.

(3) 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.

Investigation by Regulator

73. (1) The Regulator, after receipt of a complaint made in terms of section 71, must—

(a) investigate any alleged interference with the protection of the personal information of a data subject in the prescribed manner;

(b) act, where appropriate, as conciliator in relation to any such interference in the prescribed manner; and

(c) take such further action as is contemplated by this Chapter.

(2) The Regulator may, on its own initiative, commence an investigation under subsection (1).

Action on receipt of complaint

74. (1) On receiving a complaint in terms of section 71, the Regulator may—

(a) investigate the complaint; or

(b) decide, in accordance with section 75, to take no action on the complaint.

(2) The Regulator must, as soon as is reasonably practicable, advise the complainant and the responsible party to whom the complaint relates of the course of action that the Regulator proposes to adopt under subsection (1).

Regulator may decide to take no action on complaint

75. (1) The Regulator, after investigating a complaint received in terms of section 71, may decide to take no action or, as the case may be, require no further action in respect of the complaint if, in the Regulator's opinion—

(a) the length of time that has elapsed between the date when the subject matter of the complaint arose and the date when the complaint was made is such that an investigation of the complaint is no longer practicable or desirable;

(b) the subject matter of the complaint is trivial;

(c) the complaint is frivolous or vexatious or is not made in good faith;

(d) the complainant does not desire that action be taken or, as the case may be, continued;

(e) the complainant does not have a sufficient personal interest in the subject matter of the complaint; or

(f) in cases where the complaint relates to a matter in respect of which a code of conduct is in force and the code of conduct makes provision for a complaints procedure, the complainant has failed to pursue, or to pursue fully, an avenue of redress available under that complaints procedure that it would be reasonable for the complainant to pursue.

(2) Notwithstanding anything in subsection (1), the Regulator may in its discretion decide not to take any further action on a complaint if, in the course of the investigation of the complaint, it appears to the Regulator that, having regard to all the circumstances of the case, any further action is unnecessary or inappropriate.

(3) In any case where the Regulator decides to take no action, or no further action, on a complaint, the Regulator must inform the complainant of that decision and the reasons for it.

Referral of complaint to regulatory body

76. (1) If, on receiving a complaint in terms of section 71, the Regulator considers that the complaint relates, in whole or in part, to a matter that is more properly within the jurisdiction of another regulatory body, the Regulator must forthwith determine whether the complaint should be dealt with, in whole or in part, under this Act after consultation with the body concerned.

(2) If the Regulator determines that the complaint should be dealt with by another body, the Regulator must forthwith refer the complaint to that body to be dealt with accordingly and must notify the complainant of the referral.

Pre-investigation proceedings of Regulator

77. Before proceeding to investigate any matter in terms of this Chapter, the Regulator must, in the prescribed manner, inform—

(a) the complainant, the data subject to whom the investigation relates (if not the complainant) and any person alleged to be aggrieved (if not the complainant), of the Regulator's intention to conduct the investigation; and

(b) the responsible party to whom the investigation relates of the—

(i) details of the complaint or, as the case may be, the subject matter of the investigation; and

(ii) right of that responsible party to submit to the Regulator, within a reasonable period, a written response in relation to the complaint or, as the case may be, the subject matter of the investigation.

Settlement of complaints

78. If it appears from a complaint, or any written response made in relation to a complaint under section 77*(b)*(ii), that it may be possible to secure—

(a) a settlement between any of the parties concerned; and

(b) if appropriate, a satisfactory assurance against the repetition of any action that is the subject matter of the complaint or the doing of further actions of a similar kind by the person concerned,

the Regulator may, without investigating the complaint or, as the case may be, investigating the complaint further, in the prescribed manner, use its best endeavours to secure such a settlement and assurance.

Investigation proceedings of Regulator

79. For the purposes of the investigation of a complaint the Regulator may—

(a) summon and enforce the appearance of persons before the Regulator and compel them to give oral or written evidence on oath and to produce any records and things that the Regulator considers necessary to investigate the complaint, in the same manner and to the same extent as the High Court;

(b) administer oaths;

(c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Regulator sees fit, whether or not it is or would be admissible in a court of law;

(d) at any reasonable time, subject to section 80, enter and search any premises occupied by a responsible party;

(e) converse in private with any person in any premises entered under section 82 subject to section 80; and

(f) otherwise carry out in those premises any inquiries that the Regulator sees fit in terms of section 80.

Issue of warrants

80. (1) A judge of the High Court, a regional magistrate or a magistrate, if satisfied by information on oath supplied by the Regulator that there are reasonable grounds for suspecting that—

(a) a responsible party is interfering with the protection of the personal information of a data subject; or

(b) an offence under this Act has been or is being committed,

and that evidence of the contravention or of the commission of the offence is to be found on any premises specified in the information, that are within the jurisdiction of that judge or magistrate, may, subject to subsection (2), grant a warrant to enter and search such premises.

(2) A warrant issued under subsection (1) authorises the Regulator or any of its officers or staff, subject to section 82, at any time within seven days of the date of the warrant to enter the premises as identified in the warrant, to search them, to inspect,

examine, operate and test any equipment found there which is used or intended to be used for the processing of personal information and to inspect and seize any record, other material or equipment found there which may be such evidence as is mentioned in that subsection.

Requirements for issuing of warrant

81. (1) A judge or magistrate must not issue a warrant under section 80 unless satisfied that—

(a) the Regulator has given seven days' notice in writing to the occupier of the premises in question demanding access to the premises;

(b) either—

(i) access was demanded at a reasonable hour and was unreasonably refused; or

(ii) although entry to the premises was granted, the occupier unreasonably refused to comply with a request by any of the Regulator's members or officers or staff to permit the members or the officer or member of staff to do any of the things referred to in section 80(2); and

(c) that the occupier, has, after the refusal, been notified by the Regulator of the application for the warrant and has had an opportunity of being heard on the question whether the warrant should be issued.

(2) Subsection (1) does not apply if the judge or magistrate is satisfied that the case is one of urgency or that compliance with that subsection would defeat the object of the entry.

(3) A judge or magistrate who issues a warrant under section 80 must also issue two copies of it and certify them clearly as copies.

Execution of warrants

82. (1) A police officer who is assisting a person authorised to conduct an entry and search in terms of a warrant issued under section 80 may overcome resistance to the entry and search by using such force as is reasonably necessary.

(2) A warrant issued under this section must be executed at a reasonable hour unless it appears to the person executing it that there are reasonable grounds for suspecting that the evidence in question would not be found if it were so executed.

(3) If the person who occupies the premises in respect of which a warrant is issued under section 80 is present when the warrant is executed, he or she must be shown the warrant and supplied with a copy of it, and if that person is not present a copy of the warrant must be left in a prominent place on the premises.

(4) A person seizing anything in pursuance of a warrant under section 80 must give a receipt to the occupier or leave the receipt on the premises.

(5) Anything so seized may be retained for as long as is necessary in all circumstances but the person in occupation of the premises in question must be given a copy of any documentation that is seized if he or she so requests and the person executing the warrant considers that it can be done without undue delay.

(6) A person authorised to conduct an entry and search in terms of section 80 must be accompanied and assisted by a police officer.

(7) A person who enters and searches any premises under this section must conduct the entry and search with strict regard for decency and order, and with regard to each person's right to dignity, freedom, security and privacy.

(8) A person who enters and searches premises under this section must before questioning any person—

(a) advise that person of the right to be assisted at the time by an advocate or attorney; and

(b) allow that person to exercise that right.

(9) No self-incriminating answer given or statement made to a person who conducts a search in terms of a warrant issued under section 80 is admissible as evidence against the person who gave the answer or made the statement in criminal proceedings, except in criminal proceedings for perjury or in which that person is tried for an offence contemplated in section 97 and then only to the extent that the answer or statement is relevant to prove the offence charged.

Matters exempt from search and seizure

83. If the Regulator has authorised the processing of personal information in terms of section 34, that information is not subject to search and seizure empowered by a warrant issued under section 80.

Communication between legal adviser and client exempt

84. (1) Subject to the provisions of this section, the powers of search and seizure conferred by a warrant issued under section 80 must not be exercised in respect of—

(a) any communication between a professional legal adviser and his or her client in connection with the giving of legal advice to the client with respect to his or her obligations, liabilities or rights; or

(b) any communication between a professional legal adviser and his or her client, or between such an adviser or his or her client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act, including proceedings before a court, and for the purposes of such proceedings.

(2) Subsection (1) applies also to—

(a) any copy or other record of any such communication as is mentioned therein; and

(b) any document or article enclosed with or referred to in any such communication if made in connection with the giving of any advice or, as the case may be, in connection with or in contemplation of and for the purposes of such proceedings as are mentioned therein.

Objection to search and seizure

85. If the person in occupation of any premises in respect of which a warrant is issued under this Act objects to the inspection or seizure under the warrant of any material on the ground that it—

(a) contains privileged information and refuses the inspection or removal of such article or document, the person executing the warrant or search must, if he or she is of the opinion that the article or document contains information that has a bearing on the investigation and that such information is necessary for the investigation, request the Registrar of the High Court which has jurisdiction or his or her delegate to attach and remove that article or document for safe custody until a court of law has made a ruling on the question whether the information concerned is privileged or not; or

(b) consists partly of matters in respect of which those powers are not exercised, he or she must, if the person executing the warrant so requests, furnish that person with a copy of so much of the material as is not exempt from those powers.

Return of warrants

86. A warrant issued under section 80 must be returned to the court from which it was issued—

(a) after being executed; or

(b) if not executed within the time authorised for its execution,

and the person who has executed the warrant must make an endorsement on it stating what powers have been exercised by him or her under the warrant.

Assessment

87. (1) The Regulator, on its own initiative, or at the request by or on behalf of the responsible party, data subject or any other person must make an assessment in the manner prescribed of whether an instance of processing of personal information complies with the provisions of this Act.

(2) The Regulator must make the assessment if it appears to be appropriate, unless, where the assessment is made on request, the Regulator has not been supplied with such information as it may reasonably require in order to—

(a) satisfy itself as to the identity of the person making the request; and

(b) enable it to identify the action in question.

(3) The matters to which the Regulator may have regard in determining whether it is appropriate to make an assessment include the extent to which the request appears to it to raise a matter of substance, and if the assessment is made on request—

(a) any undue delay in making the request; and

(b) whether or not the person making the request is entitled to make an application,

under Principle 8 in respect of the personal information in question.

(4) If the Regulator has received a request under this section it must notify the requester—

(a) whether it has made an assessment as a result of the request; and

(b) to the extent that it considers appropriate, having regard in particular to any exemption from Principle 8 applying in relation to the personal information concerned, of any view formed or action taken as a result of the request.

Information notice

88. (1) If the Regulator—

(a) has received a request under section 87 in respect of any processing of personal information; or

(b) reasonably requires any information for the purpose of determining whether the responsible party has interfered or is interfering with the personal information of a data subject,

the Regulator may serve the responsible party with an information notice requiring the responsible party to furnish the Regulator, within a specified period, in a form specified in the notice, with an independent auditor's report indicating that the processing is taking place in compliance with the provisions of the Act, or with such information relating to the request or to compliance with the Act as is so specified.

(2) An information notice must contain particulars of the right of appeal conferred by section 92, and—

(a) in a case falling within subsection (1)*(a)*, a statement that the Regulator has received a request under section 87 in relation to the specified processing; or

(b) in a case falling within subsection (1)*(b)*, a statement that the Regulator regards the specified information as relevant for the purpose of determining whether the responsible party has complied, or is complying, with the information protection principles and the reasons for regarding it as relevant for that purpose.

(3) Subject to subsection (5), the period specified in an information notice must not expire before the end of the period within which an appeal can be brought against the notice and, if such an appeal is brought, the information need not be furnished pending the determination or withdrawal of the appeal.

(4) If the Regulator considers that the information is required as a matter of urgency, it may include in the notice a statement to that effect and a statement of its reasons for reaching that conclusion, and in that event subsection (3) does not apply.

(5) A notice in terms of subsection (4) may not require the information to be furnished before the end of a period of three days beginning with the day on which the notice is served.

(6) An information notice may not require a responsible party to furnish the Regulator with any communication between a—

(a) professional legal adviser and his or her client in connection with the giving of legal advice on the client's obligations, liabilities or rights under this Act; or

(b) professional legal adviser and his or her client, or between such an adviser or his or her client and any other person, made in connection with or in contemplation of proceedings under or arising out of this Act (including proceedings before a court) and for the purposes of such proceedings.

(7) In subsection (6) references to the client of a professional legal adviser include any person representing such a client.

(8) An information notice may not require a responsible party to furnish the Regulator with information that would, by revealing evidence of the commission of any offence other than an offence under this Act, expose the responsible party to criminal proceedings.

(9) The Regulator may cancel an information notice by written notice to the responsible party on whom it was served.

(10) After completing the assessment referred to in section 87 the Regulator—

(a) must report to the responsible party the results of the assessment and any recommendations that the Regulator considers appropriate; and

(b) may, in appropriate cases, require the responsible party, within a specified time, to inform the Regulator of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken.

(11) The Regulator may make public any information relating to the personal information management practices of a responsible party that has been the subject of an assessment under this section if the Regulator considers it in the public interest to do so.

(12) A report made by the Regulator under subsection (10) is deemed to be the equivalent of an enforcement notice in terms of section 90.

Parties to be informed of developments during and result of investigation

89. If an investigation is made following a complaint, and—

(a) the Regulator believes that no interference with the protection of the personal information of a data subject has taken place and therefore does not serve an enforcement notice;

(b) an enforcement notice is served in terms of section 90;

(c) a served enforcement notice is cancelled in terms of section 91;

(d) an appeal is lodged against the enforcement notice for cancellation or variation of the notice in terms of section 92; or

(e) an appeal against an enforcement notice is allowed, the notice is substituted or the appeal is dismissed in terms of section 93,

the Regulator must inform the complainant and the responsible party, as soon as reasonably practicable, in the manner prescribed of any development mentioned in paragraphs *(a)* to *(e)* and the result of the investigation.

Enforcement notice

90. (1) If the Regulator is satisfied that a responsible party has interfered or is interfering with the protection of the personal information of a data subject, the Regulator may serve the responsible party with an enforcement notice requiring the responsible party to do either or both of the following:

(a) To take specified steps within a period specified in the notice, or to refrain from taking such steps; or

(b) to stop processing personal information specified in the notice, or to stop processing personal information for a purpose or in a manner specified in the notice within a period specified in the notice.

(2) An enforcement notice must contain—

(a) a statement indicating the nature of the interference with the protection of the personal information of the data subject and the reasons for reaching that conclusion; and

(b) particulars of the rights of appeal conferred by section 92.

(3) Subject to subsection (4), an enforcement notice may not require any of the provisions of the notice to be complied with before the end of the period within which an appeal may be brought against the notice and, if such an appeal is brought, the notice need not be complied with pending the determination or withdrawal of the appeal.

(4) If the Regulator considers that an enforcement notice should be complied with as a matter or urgency it may include in the notice a statement to that effect and a statement of its reasons for reaching that conclusion, and in that event subsection (3) does not apply.

(5) A notice in terms of subsection (4) may not require any of the provisions of the notice to be complied with before the end of a period of three days beginning with the day on which the notice is served.

Cancellation of enforcement notice

91. (1) A responsible party on whom an enforcement notice has been served may, at any time after the expiry of the period during which an appeal may be brought against that notice, apply in writing to the Regulator for the cancellation or variation of that notice on the ground that, by reason of a change of circumstances, all or any of the

provisions of that notice need not be complied with in order to ensure compliance with the information protection principles.

(2) If the Regulator considers that all or any of the provisions of an enforcement notice need not be complied with in order to ensure compliance with the information protection principle or principles to which it relates, it may cancel or vary the notice by written notice to the responsible party on whom it was served.

Right of appeal

92. (1) A responsible party on whom an information or enforcement notice has been served may, within 30 days of receiving the notice, appeal to the High Court having jurisdiction for the setting aside or variation of the notice.

(2) A complainant, who has been informed of the result of the investigation in terms of section 75(3) or 91, may, within 30 days of receiving the result, appeal to the High Court having jurisdiction against the result.

Consideration of appeal

93. (1) If in an appeal under section 92 the court considers—

(a) that the notice against which the appeal is brought is not in accordance with the law; or

(b) that the notice involved an exercise of discretion by the Regulator that ought to have been exercised differently,

the court must allow the appeal and may set aside the notice or substitute such other notice or decision as should have been served or made by the Regulator.

(2) In such an appeal, the court may review any determination of fact on which the notice in question was based.

Civil remedies

94. (1) A data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act referred to in section 70, whether or not there is intent or negligence on the part of the responsible party.

(2) In the event of a breach the responsible party may raise any of the following defences against an action for damages:

(a) *Vis maior*;

(b) consent of the plaintiff;

(c) fault on the part of the plaintiff;

(d) compliance was not reasonably practicable in the circumstances of the particular case; or

(e) the Regulator authorised the breach in terms of section 34.

(3) A court hearing proceedings in terms of subsection (1) may award an amount that is just and equitable, including—

(a) payment of damages as compensation for patrimonial and non-patrimonial loss suffered by a data subject as a result of breach of the provisions of this Act;

(b) aggravated damages, in a sum determined in the discretion of the Court;

(c) interest; and

(d) costs of suit on such scale as may be determined by the Court.

(4) Any amount awarded to the Regulator in terms of subsection (3) must be dealt with in the following manner:

(a) The full amount must be deposited into a specifically designated trust account established by the Regulator with an appropriate financial institution;

(b) as a first charge against the amount, the Regulator may recover all reasonable expenses incurred in bringing proceedings at the request of a data subject in terms of subsection (1) and in administering the distributions made to the data subject in terms of subsection (5); and

(c) the balance, if any (in this section referred to as the ''distributable balance''), must be distributed by the Regulator to the data subject at whose request the proceedings were brought.

(5) Any amount not distributed within three years from the date of the first distribution of payments in terms of subsection (2), accrue to the Regulator in the Regulator's official capacity.

(6) The distributable balance must be distributed on a pro rata basis to the data subject referred to in subsection (1).

(7) A Court issuing any order under this section must order it to be published in the *Gazette* and by such other appropriate public media announcement as the Court considers appropriate.

(8) Any civil action instituted under this section may be withdrawn, abandoned or compromised, but any agreement or compromise must be made an order of Court.

(9) If civil action has not been instituted, any agreement or settlement, if any, may, on application to the Court by the Regulator after due notice to the other party, be made an order of Court and must be published in the *Gazette* and by such other public media announcement as the Court considers appropriate.

CHAPTER 11

OFFENCES AND PENALTIES

Obstruction of Regulator

95. Any person who hinders, obstructs or unlawfully influences the Regulator or any person acting on behalf of or under the direction of the Regulator in the performance of the Regulator's duties and functions under this Act, is guilty of an offence.

Breach of confidentiality

96. Any person who contravenes the provisions of section 47 is guilty of an offence.

Obstruction of execution of warrant

97. Any person who—

(a) intentionally obstructs a person in the execution of a warrant issued under section 80; or

(b) fails without reasonable excuse to give any person executing such a warrant such assistance as he or she may reasonably require for the execution of the warrant,

is guilty of an offence.

Failure to comply with enforcement or information notices

98. (1) A responsible party which fails to comply with an enforcement notice served in terms of section 90, is guilty of an offence.

(2) A responsible party which, in purported compliance with an information notice—

(a) makes a statement knowing it to be false; or

(b) recklessly makes a statement which is false, in a material respect,

is guilty of an offence.

Penal sanctions

99. Any person convicted of an offence in terms of this Act, is liable—

(a) in the case of a contravention of section 95, to a fine or to imprisonment for a period not exceeding 10 years, or to both a fine and imprisonment; or

(b) in any other case, to a fine or to imprisonment for a period not exceeding 12 months, or to both a fine and imprisonment.

Magistrate's Court jurisdiction to impose penalties

100. Despite anything to the contrary contained in any other law, a Magistrate's Court has jurisdiction to impose any penalty provided for in section 99.

CHAPTER 12

GENERAL PROVISIONS

Repeal and amendment of laws

101. The laws mentioned in the Schedule are amended to the extent indicated in the third column of the Schedule.

Regulations

102. The Minister may make regulations on—

(a) any matter which this Act requires or permits to be prescribed;

(b) the monitoring of this Act and the establishment of the Regulator; and

(c) any other matter which may be necessary for the application of this Act.

Transitional arrangements

103. (1) Processing which is taking place on the date when this Act comes into force and does not conform to it must, within one year of such date, be made to conform and thereafter be notified to the Regulator in terms of section 17(1).

(2) The period of one year referred to in subsection (1) may be extended by the Minister by notice in the *Gazette* to a maximum of three years.

(3) Section 56(2) does not apply to processing referred to in section 55, which is taking place on the date of commencement of this Act, or as the case may be, of the legislation, regulations or codes of conduct applying to such processing.

Short title and commencement

104. (1) This Act is called the Protection of Personal Information Act, 2009, and commences on a date determined by the President by proclamation in the *Gazette*.

(2) Different dates of commencement may be determined in respect of different provisions of this Act or in respect of different class or classes of information and bodies.

SCHEDULE

LAWS REPEALED OR AMENDED BY SECTION 101

No. and year of law	Short title	Extent of repeal or amendment
Act 2 of 2000	Promotion of Access to Information Act, 2000	**1.** The amendment of section 1 by the substitution for the definition of ''personal information'' of the following definition: **"'personal information'** means information relating to an identifiable natural 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, email address, physical address, telephone number or other particular assigned to the person; *(d)* the blood type or any other 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, but excludes information about an individual who has been dead for more than 20 years.''. **2.** The amendment of section 1 by the insertion after the definition of ''record'' of the following definition: **"'Regulator'** means the Information Protection Regulator established in terms of section 35 of the Protection of Personal Information Act, 2009.''. **3.** The amendment of section 11 by the substitution for subsection (2) of the following subsection: ''(2) A request contemplated in subsection (1) **[includes]** excludes a request for access to a record containing personal information about the requester.''.

No. and year of law	Short title	Extent of repeal or amendment
		4. The amendment of section 22 by the substitution for— *(a)* subsection (1) of the following subsection: ''(1) The information officer of a public body to whom a request for access is made, must by notice require the requester**[, other than a personal requester,]** to pay the prescribed request fee (if any), before further processing the request.''; and *(b)* subsection (2) of the following subsection: ''(2) If— *(a)* the search for a record of a public body in respect of which a request for access by a requester**[, other than a personal requester,]** has been made; and *(b)* the preparation of the record for disclosure (including any arrangements contemplated in section 29(2)*(a)* and *(b)*(i) and (ii)*(aa)*), would, in the opinion of the information officer of the body, require more than the hours prescribed for this purpose for requesters, the information officer must by notice require the requester**[, other than a personal requester,]** to pay as a deposit the prescribed portion (being not more than one third) of the access fee which would be payable if the request is granted.''. **5.** The amendment of section 54 by the substitution for— *(a)* subsection (1) of the following subsection: ''(1) The head of a private body to whom a request for access is made must by notice require the requester**[, other than a personal requester,]** to pay the prescribed request fee (if any), before further processing the request.''; and *(b)* subsection (2) of the following subsection: ''(2) If— *(a)* the search for a record of a private body in respect of which a request for access by a requester **[, other than a personal requester,]** has been made; and *(b)* the preparation of the record for disclosure (including any arrangements contemplated in section 29(2)*(a)* and *(b)*(i) and (ii)*(aa)*), would, in the opinion of the head of the private body concerned, require more than the hours prescribed for this purpose for requesters, the head must by notice require the requester**[, other than a personal requester,]** to pay as a deposit the prescribed portion (being not more than one third) of the access fee which would be payable if the request is granted.''.

No. and year of law	Short title	Extent of repeal or amendment
		6. The amendment of the heading of Part 5 by substituting the words ''Human Rights Commission'' with the words ''Information Protection Regulator''. **7.** The amendment of sections 1, 10, 32, 83, 84 and 85 by substituting the words ''Human Rights Commission'', wherever they occur, with the word ''Regulator''. **8.** The repeal of section 88.
Act 25 of 2002	Electronic Communications and Transactions Act	**1.** The amendment of section 1 by the substitution for the definition of ''personal information'' of the following definition: **'' 'personal information'** means information relating to an identifiable natural 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, email address, physical address, telephone number or other particular assigned to the person; *(d)* the blood type or any other 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, but excludes information about an individual who has been dead for more than 20 years.''. **2.** The repeal of sections 45, 50 and 51.

No. and year of law	Short title	Extent of repeal or amendment
Act 34 of 2005	National Credit Act	**1.** The amendment of section 55 by the substitution for subsection (2) of the following subsection: ''(2) *(a)* Before issuing a notice in terms of subsection (1)*(a)* to a regulated financial institution, the National Credit Regulator must consult with the regulatory authority that issued a licence to that regulated financial institution. *(b)* The information protection provisions as set out in sections 68 and 70(1) to (4) will be subject to the compliance procedures set out in Chapters 10 and 11 of the Protection of Personal Information Act, 2009.''.

MEMORANDUM ON THE OBJECTS OF THE PROTECTION OF PERSONAL INFORMATION BILL, 2009

1. PURPOSE OF BILL

The Protection of Personal Information Bill, 2009 (the Bill), emanates from the South African Law Reform Commission's report on privacy and data protection. The Bill aims to give effect to the right to privacy, by introducing measures to ensure that the personal information of an individual (data subject) is safeguarded when it is processed by responsible parties. The Bill also aims to balance the right to privacy against other rights, particularly the right of access to information, and to generally protect important interests, including the free flow of information within and across the borders of the Republic.

2. OBJECTS OF BILL

2.1 The Bill is divided into 12 Chapters and a number of the Chapters of the Bill are further subdivided into different Parts.

2.2 Chapter 1 of the Bill contains two clauses dealing with ''definitions'' and the ''purpose'' of the Bill, respectively. Clause 2 provides that the purpose of the Bill is to—

(i) protect the right to privacy with regard to the processing of personal information; and

(ii) balance the right to privacy against other rights, such as the right of access to information.

2.3 Chapter 2 reflects those provisions dealing with the application of the Act. Clause 3 clarifies that the Bill applies to the processing of personal information by or on behalf of a responsible party. A ''responsible party'' is defined as a public or private body or any other person who, alone or in conjunction with others, determines the purpose of and means for processing personal information. Clause 3 further provides that the Bill applies to the processing of personal information where the responsible party is domiciled in the Republic or where the responsible party is not domiciled in South Africa, but makes use of automated or non-automated means that are situated in the Republic.

2.4 The wide ambit of clause 3 necessitates certain exclusions, which in certain instances are qualified, as far as its application is concerned. Clause 4 provides that the Bill does not apply to the processing of personal information in the following circumstances:

(i) Personal or household activities;

(ii) de-identified information (i.e. information that had deletions effected in such a manner that the identification of the data subject is not possible);

(iii) the processing of personal information carried out in the interests of national security, defence or public safety or the prevention, investigation or proof of offences;

(iv) the processing of personal information for exclusively journalistic purposes;

(v) information processing by the Cabinet and its committees, the Executive Council of a province and a Municipal Council of a municipality;

(vi) information processing relating to the judicial functions of a court referred to in section 166 of the Constitution of the Republic of South Africa, 1996; and

(vii) the processing of personal information that has been exempted from the application of the information protection principles that are contained in the Bill.

2.5 Clause 5 establishes the principle that the Bill does not affect the operation of any other legislation that regulates the processing of personal information

and is capable of operating concurrently with the Bill. Clause 6 provides that the Bill binds all public and private bodies.

2.6.1 Chapter 3 deals with conditions for lawful processing of personal information. Part A of the Chapter reflects eight core information protection principles, namely, accountability, processing limitation, purpose specification, further processing limitation, information quality, openness, security safeguards and data subject participation. The aforementioned principles give effect to internationally accepted information protection principles which ensure that the Bill prescribes the minimum requirements for lawful processing of personal information.

2.6.2 The Bill, among others, draws a distinction between personal information and special personal information. Part B of Chapter 3 therefore regulates the processing of special personal information and places a prohibition on the processing of special personal information by responsible parties (i.e. public or private bodies). The term ''special personal information'' is defined in clause 25 as information concerning—

(i) a child who is subject to parental control in terms of the law; or

(ii) a data subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sexual life, or criminal behaviour.

2.6.3 The general prohibition in respect of the processing of special personal information is subject to a number of exceptions reflected in clauses 26 to 32. The general trend of the aforementioned exceptions can be explained with reference to a few clauses. Clause 26 creates certain exemptions in respect of the processing of special personal information concerning a data subject's religious or philosophical beliefs if such processing is carried out by spiritual or religious organisations in respect of their members. Clause 28 provides that a trade union, of which the data subject is a member, may process the information concerned if such processing is necessary to achieve the aims of the trade union. Clause 30 provides, among others, that special personal information regarding a data subject's health or sexual life may be processed by medical professionals, healthcare institutions or social services if such processing is necessary for the proper treatment and care of the data subject.

2.7 Chapter 4 contains exemptions from the information protection principles. Clause 33 provides that processing of personal information will not be in breach of the information protection principles if the Information Protection Regulator (to be established in terms of Chapter 5 of the Bill) authorises such processing. Clause 34 provides that the Regulator may authorise a responsible party to process personal information, even if that processing is in breach of an information protection principle if the Regulator is satisfied that, in the circumstances of the case—

(i) the public interest in the processing outweighs, to a substantial degree, any interference with the privacy of the data subject that could result from the processing; or

(ii) the processing involves a clear benefit to the data subject or a third party that outweighs, to a substantial degree, any interference with the privacy of the data subject or third party that could result from the processing.

2.8.1 Part A of Chapter 5 regulates matters dealing with the establishment of the Regulator (clause 35) as an independent statutory authority. This Chapter contains provisions dealing with the constitution of the Regulator and period of office of the members thereof (clause 36); the remuneration, allowances, benefits and privileges of such members (clause 37); the Secretary and staff of the Regulator (clause 38); committees of the Regulator (clause 39); meetings of the Regulator (clause 40); funding of the Regulator (clause 41); protection of the Regulator (clause 42); and the powers and duties of the Regulator (clause 43). The Regulator is, among others, empowered to monitor and enforce compliance by public and private bodies with the provisions of the Bill. The Regulator is also responsible for issuing codes of

conduct for different sectors and to make guidelines to assist bodies with the development and application of codes of conduct. Clause 44 aims to require that the Regulator must have due regard to certain matters (for example the protection of all rights and interests that compete with the right to privacy) in the performance of its functions and the exercise of its powers. Clauses 45 to 47 deal with programmes of the Regulator, reporting by the Regulator and the duty of confidentiality, respectively.

2.8.2 Part B of Chapter 5 consists of two clauses which regulate the duties and responsibilities of information protection officers and the designation of deputy information protection officer, respectively. Information protection officers are, in terms of clause 48, among others, responsible for dealing with requests that are made to the public or private bodies in terms of the Bill. These officers are required to ensure that the public or private bodies of which they are the information protection officers comply with the provisions of the Bill. Clause 49 makes provision for the designation by public and private bodies of deputy information protection officers to perform those duties contemplated in clause 48. The procedure for the designation of deputy information protection officers is regulated in terms of section 17 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000).

2.9.1 Chapter 6, which regulates ''notification'' (Part A) and ''prior investigation'' (Part B), relates to two information protection principles contained in Chapter 3, namely, Principles 3 (purpose specification) and 6 *(openness)*. Clause 50 places an obligation on responsible parties to notify the Regulator before they commence with the processing of personal information. Clause 51 prescribes the particulars, such as the name and address of the responsible party, the purpose of the processing and a description of the categories of data subjects and of the information or categories of information relating thereto, that must be contained in the notification. Clause 52 deals with the exemption in respect of the notification requirement. This clause provides that the Regulator is empowered to exempt certain categories of information processing from the notification requirement. The Regulator must, in terms of clause 53, maintain a register of all notices which he or she must make available to the public. An offence is created in terms of clause 54 in respect of any failure to comply with the notification requirement as stipulated in terms of clause 50.

2.9.2 Part B of Chapter 6 regulates prior investigations. Clause 55 requires that the Regulator must initiate an investigation before any processing commences. This requirement will be applicable where a responsible party intends, for example, to process information in respect of criminal behaviour on behalf of third parties or for the purposes of credit reporting. Clause 56 regulates matters relating to the prior investigation requirement. This clause, among others, provides that responsible parties may not carry out information processing until the Regulator has completed his or her investigation.

2.10 Chapter 7 introduces Codes of Conduct. The development of codes of conduct (code or codes) will contribute to the proper implementation of the information protection principles, as reflected in Chapter 3 of the Bill, in each sector. Clause 57, among others, provides that a code must prescribe how the information protection principles are to be complied with within specific sectors as far as the processing of personal information is concerned. The remainder of the clauses provide for the following:

(i) The Regulator may issue codes on his or her own initiative or on application by persons who process personal information (clause 58). Provision is also made in subsection (1) for stakeholder involvement and consultation in the issuing of a code.

(ii) The Regulator must, after a code is issued, publish a notice in the *Gazette* indicating that a code has been issued and where copies thereof are available. A code will come into operation 28 days after publication of the notice (clause 59).

(iii) The Regulator may from time to time amend or revoke a code that has been issued under clause 57 (clause 60).

(iv) A code may prescribe procedures for making and dealing with complaints alleging a breach of the code. If a code sets out procedures for making and dealing with complaints, the Regulator must be satisfied that the procedures meet the prescribed standards and any guidelines that may have been issued by the Regulator (clause 61).

(v) The Regulator may provide written guidelines to assist bodies to develop codes or to apply approved codes (clause 62).

(vi) The Regulator must keep a register of approved codes (clause 63).

(vii) The Regulator may, on his or her own initiative, review the operation of an approved code (clause 64).

(viii) Failure to comply with a code is deemed to be a breach of an information protection principle (clause 65).

2.11 Chapter 8 regulates the rights of persons in respect of unsolicited electronic communication and automated decision making. Some forms of direct marketing are, or have the capacity to be, more intrusive than others. The three clauses reflected in Chapter 8 therefore regulate matters relating to ''unsolicited electronic communications'' (clause 66), ''directories'' (clause 67) and ''automated decision making'' (clause 68). The general principle contained in this Chapter is that if a data subject does not respond to a responsible party's invitation to make use of its direct marketing advances, the responsible party will not be allowed to contact the consumer for a second time.

2.12 Chapter 9 consists of one provision and aims to regulate transfers of personal information outside the Republic. The flow of information across our borders benefits both organisations and individuals by lowering costs, increasing efficiency and improving customer convenience. However, the flow of personal information leads to concerns about privacy and present new challenges with respect to protecting individuals' personal information. Clause 69 therefore stipulates that information will not be transferred to another country if proper safeguards for the protection of the information have not been adopted in that country.

2.13.1 Chapter 10 provides for complaints to be lodged with the Regulator by data subjects regarding any interference with the protection of their personal information. Interference with the protection of the personal information of a data subject consist, in terms of clause 70, of—

(i) any breach of the information protection principles set out in Chapter 3 of the Bill;

(ii) non-compliance with any obligations created in terms of the Bill; or

(iii) a breach of the provisions of a code that has been issued in terms of clause 57.

2.13.2 The remaining provisions of the Chapter deal with the powers of the Regulator as far as investigation of complaints are concerned and aim to regulate the following:

(i) Clauses 71 and 72 provide that complaints may be submitted to the Regulator regarding the interference with personal information of a data subject and the manner in which such complaints may be made, respectively.

(ii) Clauses 73 to 78 reflect those provisions dealing with the investigation of complaints by the Regulator and include matters such as the power to refer a complaint to another regulatory body if such regulatory body is in a better position to deal with the complaint. The Regulator is also required, in terms of clause 77 as part of the Regulator's proceedings that precede the investigation itself, to inform the complainant of his or her intention to conduct an investigation and to allow the responsible party the opportunity to submit a written response in respect of the complaint to the Regulator. Clause 78 provides that the Regulator may, if it is possible

to settle the dispute between the parties, do so without proceeding with or concluding an investigation.

(iii) Clauses 79 to 86 regulate the various aspects associated with the investigations conducted by the Regulator. As far as the investigation of complaints is concerned the Regulator will, among others, in terms of clause 79 be empowered to summon persons to appear before him or her, receive and accept any evidence and enter and search any premises that is occupied by a responsible party. The remaining clauses deal with procedural aspects in relation to the investigations to be conducted by the Regulator. These provisions deal with the issuing of search warrants (clause 80); the requirements for warrants to be issued (clause 81); the execution of warrants (clause 82); matters that are exempt from searches (clause 83); exemption of communication between a legal adviser and his or her client (clause 84); the possibility of objections to be raised with regard to searches (clause 85); and the return of warrants to the court that issued them after they have been executed or if they were not executed within the authorised period (clause 86).

(iv) Clauses 87 and 88 give effect to the need for assessments or audits to be conducted with regard to the processing of personal information practices in order to determine whether such practices comply with the provisions of the Bill. An assessment may, in terms of clause 87, be conducted on the Regulator's own initiative or at the request of another person. After completing the assessment the Regulator must report the results thereof to the responsible party together with an appropriate recommendation.

(v) Clause 89 requires that the Regulator must inform complainants and responsible parties of any developments in or the result of investigations.

(vi) The Regulator will also be empowered to make a determination that a responsible party must take specified action, or cease to act in a specific manner, within a specified period for the purpose of complying with the provisions of the Bill. Failure to comply with the information or enforcement notices will be a criminal offence. Clauses 90 to 93 of the Bill aim to give effect to the aforementioned.

(vii) Clause 94 provides that a court may, apart from compensatory damages for patrimonial and non-patrimonial loss, also award aggravated damages that are just and equitable.

2.14 Chapter 11 deals with offences and penalties. The Chapter, among others, creates offences such as obstruction of the Regulator (clause 95), breach of confidentiality by a person acting on behalf of a responsible party (clause 96) and the failure to comply with an enforcement notice (clause 98).

2.15 Chapter 12 reflects certain general provisions such as the amendment of certain laws (clause 101), the Minister's power to make regulations (clause 102) and the short title and commencement of the Act (clause 104). The Schedule to the Bill is intended to effect certain amendments to existing legislation, among others, to ensure that all the responsibilities of the Human Rights Commission in terms of the Promotion of Access to Information Act, 2000, are assigned to the Regulator.

3. DEPARTMENTS/BODIES/PERSONS CONSULTED

The South African Law Reform Commission consulted widely during the course of its investigation and solicited comments from a variety of interested parties in the public and private sectors.

4. IMPLICATIONS FOR PROVINCES

None.

5. FINANCIAL IMPLICATIONS FOR STATE

Approximately R17 million will be required to establish the Office of the Information Protection Regulator. Clause 41 of the Bill, among others, provides that Parliament must appropriate annually such sums of money as may be necessary for the proper exercise, performance and discharge by the Regulator of its powers, duties and functions. Funds have not yet been committed for the establishment of the Regulator.

6. PARLIAMENTARY PROCEDURE

6.1 The State Law Advisers and the Department of Justice and Constitutional Development are of the opinion that the Bill must be dealt with in accordance with the procedure established by section 75 of the Constitution since it contains no provision to which the procedure set out in section 74 or 76 of the Constitution applies.

6.2 The State Law Advisers are of the opinion that it is not necessary to refer this Bill to the National House of Traditional Leaders in terms of section 18(1)*(a)* of the Traditional Leadership and Governance Framework Act, 2003 (Act No. 41 of 2003), since it does not contain provisions pertaining to customary law or customs of traditional communities.

Printed by Creda Communications

ISBN 978-1-77037-624-3