Code of Conduct governing the Conditions for Lawful Processing of Personal Information by members of the Credit Bureau Association, South Africa.

Issued in terms of Section 60 of the Protection of Personal Information Act, No. 4 of 2013 ("PoPIA") by the Information Regulator

CODE OF CONDUCT : Lawful Processing of Personal Information in credit Sector

THE CREDIT BUREAU ASSOCIATION, SOUTH AFRICA

cba credit bureau association

Table of Contents

PART A – INTRODUCTION

1. BACKGROUND

1.1 The Credit Bureau Association, South Africa ("CBA") is a voluntary association of credit bureaux duly registered in terms of Section 43(1) of the National Credit Act, 34 of 2005 (as amended) ("NCA"), by the National Credit Regulator ("NCR").

1.2 Not all registered credit bureaux are members of the CBA. At the time of the submission of this Code of Conduct to the Information Regulator for consideration and issue of the Code of Conduct the CBA represents 10 of the 14 credit bureaux registered by the NCR.

1.3 The members of the CBA process the vast majority of consumer credit information relied upon by the credit industry in South Africa and are bound by the CBA Constitution to process consumer credit information in a manner that promotes confidentiality, accuracy and relevancy in accordance with international best practice and relevant legislation.

1.4 Credit bureaux are governed by the NCA and Regulations prescribed by the NCR in terms of the NCA ("NCA Regulations").

1.5 The NCA:

1.5.1 has as its primary purpose the advancement of the social and economic welfare of South Africans and promotes a fair, transparent, competitive, sustainable, responsible, efficient, effective and accessible credit market and industry;

1.5.2 seeks to protect consumers by, among other things, encouraging responsible borrowing, avoidance of over indebtedness and fulfilment of financial obligations by consumers. It discourages reckless credit granting by Data providers and default in the repayment to Data providers by consumers;

1.5.3 read with the NCA Regulations, requires the reporting of consumer credit information in a manner that protects the confidentiality and integrity of the information;

1.5.4 regulates credit bureaux.

1.6 The Protection of Personal Information Act, 4 of 2013 ("PoPIA") stipulates as among its primary purposes; giving effect to the constitutional right of privacy, the establishment of the manner in which personal information may be processed by prescribing minimum threshold requirements for the lawful processing of personal information and providing remedies to persons whose personal information is not lawfully processed in accordance with PoPIA.

1.7 PoPIA recognises that the provisions of the NCA governing the processing of information, and in particular confidential information (as defined in the NCA Regulations), falls within the remit of the Information Regulator, the NCA having been expressly amended in terms of PoPIA to address this stipulation. These provisions are subject to the compliance procedures governing

"Enforcement" in Chapter 10 and "Offences, Penalties and Administrative Fines" in Chapter 11 of PoPIA.

1.8 In addition to the conditions governing the lawful processing of personal information stipulated in PoPIA, credit bureaux are also subject to the restrictions contained in Section 70 of the NCA, read with Section 18 of the NCA Regulations, governing the processing of consumer credit information.

1.9 The CBA will, in the drafting of and applying to the Regulator for the issue of this Code of Conduct, consult with the NCR and the Information Regulator, with a view to promoting compliance with PoPIA and a consistency in the approach of its members in this regard.

2. MANDATE AND APPLICATION

2.1 By applying to the Information Regulator for the issue of this Code of Conduct the CBA confirms that it is acting in terms of the mandate of all of its members at the time that the application is made.

2.2 The CBA Executive Manager is mandated to, prior to the issue of this Code of Conduct, request the Information Regulator to provide rulings of interpretation on PoPIA that may affect the provisions of this Code of Conduct and to affect non-material amendments to the wording of this Code of Conduct as may be required by the Information Regulator, without further reference to CBA members.

2.3 This Code of Conduct applies to credit bureaux, who are members of the CBA, in their processing of consumer credit information (by definition in PoPIA personal information) in the course of fulfilling credit bureaux obligations in processing information for the purposes of credit reporting. This Code of Conduct does not apply to the processing of personal information in the course of the conduct and management of the business of a credit bureau.

3. PURPOSE

3.1 The purpose of this Code of Conduct is to:

3.1.1 promote appropriate practices by members of the CBA governing the processing of personal information;

3.1.2 encourage the establishment of appropriate agreements between members of the CBA and third parties, regulating the processing of personal information as required in PoPIA and dictated by good business practice.

3.2 A further purpose of this Code of Conduct is to establish procedures for members of the CBA to be guided in their interpretation of principally PoPIA, but also other law or practices governing the processing of personal information, in the interaction between credit bureaux

allowing for complaints against credit bureaux to be considered and remedial action, where appropriate, to be taken.

4. SCOPE

4.1 This Code of Conduct governs:

4.1.1 the processing of personal information (including consumer credit information) by credit bureaux that are members of the CBA in compliance with PoPIA and the NCA;

4.1.2 where appropriate, agreements that may need to be concluded between members of the CBA and third parties promoting, and to the extent possible ensuring, that personal information (including consumer credit information) is processed in compliance with PoPIA and the NCA;

4.1.3 the enforcement by the CBA of the provisions of this Code of Conduct.

4.2 The CBA must ensure that members of the CBA accept that their membership is subject to compliance with this Code of Conduct.

5. DEFINITIONS AND ABBREVIATIONS

5.1 Relevant PoPIA definitions:

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

5.1.2 ‘‘code of conduct’’ means a code of conduct issued in terms of Chapter 7 of PoPIA;

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

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

5.1.5 ‘‘Constitution’’ means the Constitution of the Republic of South Africa, 1996;

5.1.6 ‘‘data subject’’ means the person to whom personal information relates;

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

5.1.7.1 identifies the data subject;

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

5.1.7.3 can be linked by a reasonably foreseeable method to other information that identifies the data subject, and ‘‘de-identified’’ has a corresponding meaning;

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

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

5.1.8.2 requesting the data subject to make a donation of any kind for any reason;

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

5.1.10 ‘‘enforcement notice’’ means a notice issued in terms of section 95;

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

5.1.12 ‘‘information officer’’ of, or in relation to, a—

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

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

5.1.13 ‘‘Minister’’ means the Cabinet member responsible for the administration of justice;

5.1.14 ‘‘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;

5.1.15 ‘‘person’’ means a natural person or a juristic person;

5.1.16 ‘‘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—

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

5.1.16.2 information relating to the education or the medical, financial, criminal or employment history of the person;

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

5.1.16.4 the biometric information of the person;

5.1.16.5 the personal opinions, views or preferences of the person;

5.1.16.6 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;

5.1.16.7 the views or opinions of another individual about the person; and

5.1.16.8 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;

5.1.17 ‘‘prescribed’’ means prescribed by regulation or by a code of conduct;

5.1.18 ‘‘private body’’ means—

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

5.1.18.2 a partnership which carries or has carried on any trade, business or profession; or

5.1.18.3 any former or existing juristic person, but excludes a public body;

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

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

5.1.19.2 dissemination by means of transmission, distribution or making available in any other form; or

5.1.19.3 merging, linking, as well as restriction, degradation, erasure or destruction of information;

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

5.1.21 ‘‘public body’’ means—

5.1.21.1 any department of state or administration in the national or provincial sphere of government or any municipality in the local sphere of government; or

5.1.21.2 any other functionary or institution when—

5.1.21.2.1 exercising a power or performing a duty in terms of the Constitution or a provincial constitution; or

5.1.21.2.2 exercising a public power or performing a public function in terms of any legislation;

5.1.22 ‘‘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;

5.1.23 ‘‘record’’ means any recorded information—

5.1.23.1 regardless of form or medium, including any of the following:

5.1.23.1.1 Writing on any material;

5.1.23.1.2 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;

5.1.23.1.3 label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;

5.1.23.1.4 book, map, plan, graph or drawing;

5.1.23.1.5 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;

5.1.23.2 in the possession or under the control of a responsible party;

5.1.23.3 whether or not it was created by a responsible party; and

5.1.23.4 regardless of when it came into existence;

5.1.24 ‘‘Regulator’’ means the Information Regulator established in terms of section 39 of PoPIA;

5.1.25 ‘‘Republic’’ means the Republic of South Africa;

5.1.26 ‘‘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;

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

5.1.28 ‘‘special personal information’’ means personal information as referred to in section 26;

5.1.29 ‘‘this Act’’ includes any regulation or code of conduct made under the Protection of Personal Information Act, 4 of 2013; and

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

5.2 Relevant NCA definitions:

5.2.1 “agreement” includes an arrangement or understanding between or among two or more parties, which purports to establish a relationship in law between those parties;

5.2.2 “complainant” means a person who has filed a complaint in terms of section 136(1);

5.2.3 “confidential information” means personal information that belongs to a person and is not generally available to or known by others;

5.2.4 “consumer”, in respect of a credit agreement to which this Act applies, means-

5.2.4.1 the party to whom goods or services are sold under a discount transaction, incidental credit agreement or instalment agreement;

5.2.4.2 the party to whom money is paid, or credit granted, under a pawn transaction;

5.2.4.3 the party to whom credit is granted under a credit facility;

5.2.4.4 the mortgagor under a mortgage agreement;

5.2.4.5 the borrower under a secured loan;

5.2.4.6 the lessee under a lease;

5.2.4.7 the guarantor under a credit guarantee; or

5.2.4.8 the party to whom or at whose direction money is advanced or credit granted under any other credit agreement;

5.2.5 “consumer credit information” means information concerning-

5.2.5.1 a person’s credit history, including applications for credit, credit agreements to which the person is or has been a party, pattern of payment or default under any such credit agreements, debt re-arrangement in terms of this Act, incidence of enforcement actions with respect to any such credit agreement, the circumstances of termination of any such credit agreement, and related matters;

5.2.5.2 a person's financial history, including the person's past and current income, assets and debts, and other matters within the scope of that person's financial means, prospects and obligations, as defined in section 78(3), and related matters;

5.2.5.3 a person's education, employment, career, professional or business history, including the circumstances of termination of any employment, career, professional or business relationship, and related matters; or

5.2.5.4 a person's identity, including the person's name, date of birth, identity number, marital status and family relationships, past and current addresses and other contact details, and related matters.

5.2.6 "credit", when used as a noun, means-

5.2.6.1 a deferral of payment of money owed to a person, or a promise to defer such a payment; or

5.2.6.2 a promise to advance or pay money to or at the direction of another person;

5.2.7 "credit bureau" or "credit bureaux" means a person/s required to apply for registration as such in terms of section 43(1);

5.2.8 "Data provider", in respect of a credit agreement to which this Act applies, means-

5.2.8.1 the party who supplies goods or services under a discount transaction, incidental credit agreement or instalment agreement;

5.2.8.2 the party who advances money or credit under a pawn transaction;

5.2.8.3 the party who extends credit under a credit facility;

5.2.8.4 the mortgagee under a mortgage agreement;

5.2.8.5 the lender under a secured loan;

5.2.8.6 the lessor under a lease;

5.2.8.7 the party to whom an assurance or promise is made under a credit guarantee;

5.2.8.8 the party who advances money or credit to another under any other credit agreement; or

5.2.8.9 any other person who acquires the rights of a Data provider under a credit agreement after it has been entered into;

5.2.9 "credit regulator" means a provincial credit regulator or the National Credit Regulator established by section 12 of the National Credit Act, 34 of 2005 (as amended);

5.2.10 "juristic person" includes a partnership, association or other body of persons, corporate or unincorporated, or a trust if-

5.2.10.1 there are three or more individual trustees; or

5.2.10.2 the trustee is itself a juristic person, but does not include a stokvel;

5.2.11 "Magistrates' Courts Act" means the Magistrates' Courts Act, 32 of 1944;

5.2.12 "organ of state" means an organ of state as defined in section 239 of the Constitution;

5.2.13 "prescribed" means prescribed by regulation;

5.2.14 "reckless credit" means the credit granted to a consumer under a credit agreement concluded in circumstances described in section 80;

5.2.15 "NCA regulation" means a regulation made under the National Credit Act, 34 of 2005;

5.2.16 "sms" means a short message service provided through a telecommunication system;

5.3 Code of Conduct definitions:

5.3.1 "business days" means all weekdays which are not proclaimed public holidays in the Republic of South Africa;

5.3.2 "CBA Constitution" means the constitution adopted by the members of the Credit Bureau Association, South Africa and any amendments thereto;

5.3.3 "CBA Executive Manager" means the person appointed by the CBA to oversee the conduct of its business.

5.4 Abbreviations:

5.4.1 "CBA" means the Credit Bureau Association, South Africa, a voluntary association of credit bureaux duly registered in terms of Section 43 of the National Credit Act, 34 of 2005;

5.4.2 "CPA" means the Consumer Protection Act, 68 of 2008;

5.4.3 "ISMS" means an Information Security Management System;

5.4.4 "NCA" means the National Credit Act, 34 of 2005 (as amended);

5.4.5 "NCA Regulations" means the National Credit Act Regulations (as amended) prescribed by the National Credit Regulator, published in 2006;

5.4.6 "NCR" means the National Credit Regulator established in terms of Section 12 of the National Credit Act, 34 of 2005;

5.4.7 "PAIA" means the Promotion of Access to Information Act, 2 of 2000;

5.4.8 "PoPIA" means the Protection of Personal Information Act, 4 of 2013;

6. ORGANISATION OF THIS CODE

6.1 PART B of this Code of Conduct deals with each of:

6.1.1 the lawful conditions for Processing of personal information;

6.1.2 the Processing of special personal information; and

6.1.3 the Processing of personal information of children.

6.2 PART C of this Code of Conduct deals with:

6.2.1 the Duties and responsibilities of the Information Officer;

6.2.2 Direct marketing by means of unsolicited electronic communications; and

6.2.3 Transfers of personal information outside Republic.

6.3 In PARTS B and C of this Code of Conduct the relevant provisions of PoPIA are quoted in full, and are identified by being shaded.

6.4 Immediately subsequent to the provisions referred to in 6.3, reference is made to *Other Applicable Legislation* relevant to the processing of personal information by credit bureaux. These provisions are in italics.

6.5 Immediately subsequent to the provisions referred to in 6.4, *Other Applicable Legislation*, a brief commentary providing guidance to credit bureaux relating to the processing of personal information in compliance with PoPIA in terms of accepted industry practices is provided.

6.6 Immediately subsequent to the commentary, the obligations of members of the CBA to comply with PoPIA or actions or omissions that are a functional equivalent in the processing of personal information (including consumer credit information) are stipulated in bold. These provisions do not substitute the stipulations of PoPIA or in any way detract from their operation and must be construed as supplementary to the provisions of PoPIA.

7. COMMENCEMENT OF THE CODE

7.1 This Code of Conduct will come into force and be binding on every member of the CBA at the end of the grace period provided in Section 62(2) of PoPIA, which grace period will commence once the PoPIA commencement date has been effected in the Government Gazette If no grace period is granted, this Code of Conduct will come into effect and be binding on the members of the CBA on the date that PoPIA or any proclamation by the State President requires compliance with those provisions.

7.2 Notwithstanding any delays in the commencement of PoPIA or the expiry of transitional arrangements stipulated in Section 114 of PoPIA, the CBA encourages its member to ensure that the processing of personal information complies with PoPIA as early as may reasonably be achieved.

PART B – CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

8. GENERAL

8.1 PoPIA takes precedence over any other legislation that regulates the processing of personal information where that legislation is materially inconsistent with an object, or a specific provision of PoPIA, unless the other legislation regulates the processing more extensively than the conditions for lawful processing of personal information, in which event the more extensive provisions will prevail.

8.2 Chapter 3 of PoPIA stipulates the conditions for lawful processing of personal information. Codes of Conduct must incorporate these conditions or set out obligations that provide a functional equivalent to the obligations established in the conditions.

8.3 In considering the conditions for the lawful processing of personal information the separate conditions must not be considered in isolation. They should be regarded as a constellation of conditions that interact with and may influence the interpretation of the other conditions as circumstances may dictate. For example: The purpose of collecting and processing personal information will impact on whether personal information is adequate, relevant and not excessive and whether the processing of the personal information is justified. It may also impact on whether the personal information must be collected directly from a data subject and, depending on the scope of the initial purpose, whether further processing is compatible and permissible in terms of PoPIA. The Purpose specification may also influence the period for which personal information may lawfully be retained.

8.4 A further example is the requirement for Notification to a data subject where collecting personal information. This is inextricably linked to the provisions in other sections allowing a data subject to access personal information, require the amendment of incorrect personal information and object to the processing of personal information, all of which are dealt with in separate sections of PoPIA dealing with the conditions of lawful processing of personal information.

8.5 For the convenience of the reader the full text of each of the conditions for lawful processing of personal information are contained in this Code of Conduct. Definitions applicable to these provisions are also contained in the Definition section of this Code of Conduct.

8.6 Credit bureaux and other members of the credit industry are subject to governance and regulation stipulated in terms of the NCA. The NCA expressly deals with “consumer credit information” (defined in Section 70) and with “confidential information”, defined to mean *“Personal information that belongs to a person and is not generally available to or known by others”*. Both “consumer credit information” and “confidential information” as used in the NCA fall within the definition of “personal information” in PoPIA. In recognition of this PoPIA amends the NCA to provide that Sections 68, 70(1), (2)(b) to (g) and (i), (3) and (4) and 72(1), (3) and

(5) of the NCA will be subject to the compliance procedures set out in Chapters 10 and 11 of PoPIA.

8.7 It must be noted that while the general principles of processing of personal information stipulated in PoPIA apply to all personal information, the NCR shall retain its authority to deal with the filing of consumer credit information, inferences that may be drawn when no consumer credit information is available and the reporting of information in terms of Sections 70(2)(a), (h) and (i) of the NCA.

8.8 The provisions governing the processing of information in the NCA, while not as extensive as PoPIA, are not inconsistent with PoPIA and credit bureaux complying with the NCA in this regard will largely comply with the conditions for the lawful processing of personal information contained in PoPIA.

8.9 In consequence of their compliance with the NCA, credit bureaux will, in many instances, have developed practices that comply with the conditions for the lawful processing of personal information or practices that constitute functional equivalence of what is required in these conditions. To the extent that it may be appropriate, guidance is provided relating to these practices and the correlation with the conditions for the lawful processing of personal information.

8.10 All persons that are subject to this Code of Conduct, whether by virtue of membership of the CBA or by written agreement, must comply with the conditions for the lawful processing of personal information stipulated in PoPIA and/or the functional equivalents of practices in the credit industry that afford at least the same protection to data subjects as are contemplated in the conditions for the lawful processing of personal information stipulated in PoPIA.

1. CONDITION 1: ACCOUNTABILITY

Responsible party to ensure conditions for lawful processing

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

Other Applicable Legislation:

- *The NCA not being, as PoPIA is, a general law of application, does not use generic terms that correlate to responsible party and operator. Instead the responsibilities of credit bureaux and parties with whom credit bureaux may interact in the processing of consumer credit information are expressly stipulated in Sections 68, 70, 72, 73 of the NCA and Sections 17 to 19 of the NCA Regulations.*

1.1 In processing personal information it is important that credit bureaux establish in what circumstances they act as responsible parties and in what circumstances they act as operators.

1.2 By definition a "responsible party" is a person who alone or in conjunction with others, determines the purpose of and means of processing personal information.

1.3 By definition an "operator" is a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of the responsible party.

1.4 In terms of these definitions whether a credit bureau acts as a responsible party or an operator is fact dependent. A credit bureau may in certain circumstances be a responsible party, in others an operator and also where it acts in conjunction with others in determining the purpose and means for processing personal information it may act together with others as a responsible party.

1.5 In processing personal information, whether as a responsible party or an operator, a credit bureau must comply with the conditions for the lawful processing of personal information. The distinction lies in the fact that a responsible party is liable to the data subject and must ensure that all of the conditions of lawful processing of personal information and measures that give effect to these conditions are complied with. Specifically with regard to Security Safeguards in Condition 7, PoPIA requires that the responsible party must conclude a written contact with the operator and ensure that the operator establishes and maintains the security measures necessary to safeguard the integrity and confidentiality of personal information.

1.6 Credit bureaux may be assisted in establishing whether they act as responsible parties or operators by reference to the obligations imposed on them in terms of the NCA, supplemented by its Regulations.

1.7 Credit bureaux will ensure that those persons responsible for the credit bureau complying with its obligations in terms of PoPIA (including the Information Officer) are appropriately trained

to determine when the credit bureau acts as a responsible party and when it acts as an operator.

A CREDIT BUREAU MUST:

- **In processing personal information determine whether it acts as a responsible party or as an operator and it must fulfil its obligation to give effect to the conditions for the lawful processing of personal information, as may be appropriate.**

2. CONDITION 2: PROCESSING LIMITATION

Lawfulness of processing

9. Personal information must be processed—

   (a) lawfully; and

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

Other Applicable Legislation:

The NCA:

- *Requires that the National Credit Regulator register credit bureaux subject to compliance with the provisions of Section 43 of the NCA.*
- *In Sections 70(2) and (3) stipulates what a credit bureau must do in the course of conducting the business of a credit bureau.*

Unless a credit bureau is in breach of these provisions it will process personal information, including consumer credit information, lawfully. The lawfulness of credit bureaux acting as such derives from their registration in terms of the NCA and, in the context of this Code of Conduct, compliance with provisions regulating the process of consumer credit information.

2.1 Aside from lawfulness, which would include the sharing of personal information for the purposes of assessing credit and in the furtherance of the purposes of the NCA, the person processing the information (this is not restricted to the responsible party) must ensure that it is processed in a reasonable manner so as not to infringe the privacy of the data subject.

2.2 What is "reasonable"? Reasonableness assumes that all of the conditions for lawful processing are adhered to.

2.3 Further, that the data subject has knowledge of:

2.3.1 who is processing his or her personal information;

2.3.2 the intended use of the personal information; and

2.3.3 can establish the manner in which the personal information will be handled and secured.

2.4 A data subject may reasonably expect that personal information will not be processed where the processing is unjustified or where it may have an unsubstantiated negative effect on the data subject.

2.5 If credit bureaux process personal information in compliance with PoPIA and the NCA, the processing will be lawful, reasonable and will not infringe the privacy of the data subject.

A CREDIT BUREAU MUST:

- **Be registered in terms of Section 43 of the NCA;**
- **Comply with laws governing the processing of personal information;**

- **Ensure that the processing of personal information is not only lawful but reasonable and does not infringe the privacy of a data subject.**

Minimality

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

Other Applicable Legislation:

The NCA:

- *In Section 3 describes its purpose;*
- *In Section 70(1) defines "consumer credit information";*
- *In Section 70(2) stipulates how a credit bureau must process the information; and*
- *In Section 70(2)(f) requires the prompt expunging of consumer credit information that is not permitted to be entered into in its records requires to be removed from its record.*

The NCA Regulation:

- *In Section 18(3) stipulates what information may not be contained in the records of a credit bureau.*

2.6 The processing of consumer credit information is circumscribed by the NCA's purpose stipulated in section 3 and section 70 (1) that expressly defines the information that may be processed by credit bureaux.

2.7 In determining what information may be lawfully processed by credit bureaux regard must be had to the provisions of Regulation 18(3) of the NCA Regulations. This Regulation prohibits credit bureaux records from containing certain categories of consumer credit information.

2.8 Save for biometric information and information relating to alleged criminal behaviour, the categories in the NCA Regulations that a credit bureau is prohibited from processing correlate substantially to Special Personal Information, the processing of which is prohibited in terms of PoPIA unless the appropriate authorisation is obtained for the processing of the Special Personal Information.

2.9 Section 70(2)(f) requires that prescribed consumer information (which will include the information contemplated in Regulation 18(3)) must not be retained in the records of a credit bureaux and if received, must be promptly expunged. With regard to the information referred to in Regulation 18(3) of the NCA Regulations, credit bureaux must expunge, destroy or delete this information in a manner that prevents its reconstruction in an intelligible form.

2.10 There are other instances that although the Act or Regulation may require the expungement of information this has been interpreted as the logical destruction of the information. This means that the credit bureaux retain these records to allow comparison with information that may be provided at a later time. If the information is materially identical the incoming information is ignored and not captured on the credit bureaux information systems, alternatively is promptly expunged.

2.11 Thus, while definitions of expunge indicate an obliteration or permanent removal of information, to enable the proper processing of information to ensure no repetitions of the capture and processing of information that credit bureaux are prohibited from processing, it is necessary for credit bureaux to retain the information in order to make appropriate comparisons and avoid improper processing of the information.

2.12 Information that is required to be expunged is retained by the credit bureaux, but is neither displayed nor used for the purposes of credit scoring or credit assessment as contemplated in Section 17 of the NCA Regulations and must be processed subject to stringent security control measures protecting the confidentiality of the information, appropriate to satisfy the Security Safeguard requirements specified in Condition 7 of PoPIA.

2.13 In this context the provisions of the NCA are more demanding than those in PoPIA and credit bureaux must not retain ("storage" is by definition "processing") consumer credit information if it is no longer relevant or if it is excessive.

2.14 The maximum period of display of information as required in Section 17 of the NCA Regulations are more fully dealt with in paragraphs 3.4 to 3.8 dealing with the Retention and Restriction of Records in Part B of this Code of Conduct.

A CREDIT BUREAU MUST:

- **Not process personal information that is irrelevant and excessive to its functions as a credit bureaux;**
- **Where information is retained beyond the periods stipulated for it to be displayed or used for the purposes of credit scoring, but remains necessary for the processing of consumer credit information, establish and maintain appropriate security safeguards aimed at ensuring the integrity and confidentiality of the personal information retained by the credit bureau.**

Consent, justification and objection

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

(a) the data subject or a competent person where the data subject is a child consents to the processing;

(b) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

(c) processing complies with an obligation imposed by law on the responsible party;

(d) processing protects a legitimate interest of the data subject;

(e) processing is necessary for the proper performance of a public law duty by a public body; or

(f) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

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

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

(3) A data subject may object, at any time, to the processing of personal information–

(a) in terms of subsection (1)(d) to (f), in the prescribed manner, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or

(b) for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications as referred to in section 69.

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

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

Other Applicable Legislation:

The NCA:

- *In Section 3 determines the purpose of processing consumer credit information in order to promote responsibility in the credit market by encouraging responsible borrowing, the avoidance of over-indebtedness, fulfilment of financial obligations by consumers and discouraging reckless credit granting by credit providers and contractual default by consumers. A further purpose expressly stipulated is improving consumer credit information and reporting.*

2.15 A person who applies for credit will typically expressly consent to the processing of relevant personal information (consumer credit information) for the purpose of the extension of credit. Alternatively, as one of the purposes of the NCA is to encourage responsible borrowing and discourage the reckless granting of credit, the NCA places a duty on Data providers to assess the creditworthiness of applicants for credit and the necessity to conduct the necessary credit checks may be implied.

2.16 The credit bureau, in processing the consumer credit information, which by its nature is personal information, must do so in compliance with its obligations stipulated in terms of Sections 70(2) and (3) of the NCA.

2.17 In issuing a report to any person requiring it for the purposes contemplated in the NCA or prescribed in NCA Regulations, a credit bureau acts in both the legitimate interests of the data subject and the legitimate interests of the responsible party in fulfilling the stipulated purpose of the NCA, of promoting responsible borrowing and discouraging the reckless grant of credit by providing accurate credit information.

A CREDIT BUREAU MUST:

- **Process personal information strictly in the terms of obligations imposed on it by law and for no other purpose.**

Collection directly from data subject

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

(2) It is not necessary to comply with subsection (1) if—

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

(b) the data subject or a competent person where the data subject is a child has consented to the collection of the information from another source;

(c) collection of the information from another source would not prejudice a legitimate interest of the data subject;

(d) collection of the information from another source is necessary—

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

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

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

(iv) in the interests of national security; or

(v) to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;

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

(f) compliance is not reasonably practicable in the circumstances of the particular case.

Other Applicable Legislation:

The NCA stipulates:

- *In Section 70(2) that a credit bureau must accept consumer credit information from any credit provider; and in Section 70(3)(b) other prescribed persons;*

The NCA Regulations prescribe:

- *In Section 18(7) "… from any person, provided the originating source of the information is one of the following persons:*
  - *(a) An organ of state, a court or judicial officer;*
  - *(b) Any person who supplies goods, services or utilities to consumers …;*
  - *(c) A person providing long term and short term insurance;*
  - *(d) Entities involved in fraud investigation;*
  - *(e) Educational institutions;*
  - *(f) Debt collectors to whom book debt was ceded or sold by a credit provider;*
  - *(g) Other registered credit bureaus."*

2.18 If a credit bureau collects personal information, which by definition includes consumer credit information, directly from a data subject for the purpose of the conduct of its business and

reporting credit information to data subjects, the stipulations of PoPIA and in particular the lawful conditions for processing of personal information must be complied with.

2.19 If personal information, which by definition includes consumer credit information, is not collected directly from the data subject by the credit bureau but emanates from a Data provider, the credit bureau may accept that the information originates from the sources prescribed in Section 70(2) of the NCA and Section 18(7) of the NCA Regulations.

2.20 A credit bureau must accept consumer credit information from any Data provider and may accept consumer credit information that originates from sources prescribed in the NCA Regulations.

2.21 In the case of a credit bureau the collection of personal information falls within the exception in Sections 12(2)(c) and (d)(v) of PoPIA in that the collection does not prejudice the legitimate interests of the data subject and it does maintain the legitimate interests of the responsible party or the third party to whom the information is supplied.

A CREDIT BUREAU MUST:

- **Unless it collects information directly from a data subject, only collect personal information from Data providers or persons prescribed in Section 18(7) of the NCA Regulations;**
- **Conclude agreements with all persons from whom it collects personal information confirming the data subject has been notified in terms of Section 18(1) of PoPIA that the personal information will be processed by a credit bureau, alternatively where consent is expressly required in terms of PoPIA that the necessary consent has been obtained: Provided that if the information is submitted in terms of a lawful obligation, the person providing information to the credit bureau shall not be required to provide confirmation to a credit bureau that notification has been provided to the data subject;**
- **If it collects personal information directly from a data subject, before the information is collected, provide the notification to the data subject required in Section 18(1) of PoPIA.**

3. CONDITION 3: PURPOSE SPECIFICATION

Collection for specific purpose

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

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

Other Applicable Legislation:

The NCA stipulates:

- *In Section 68(1) that any person who compiles, retains or reports any confidential information in terms of the NCA must protect the information and only use that information for the purpose permitted or required in the NCA, other national legislation or provincial legislation.*

The NCA defines "confidential information" as personal information that belongs to a person and is not generally available to or known by others.

Typically personal information relating to a person's financial status or applications for credit would be regarded by the data subject as confidential.

3.1 If a credit bureaux collects information directly from a data subject it must ensure that the data subject is aware of the specific, explicitly defined and lawful purpose related to the function and activity of the credit bureaux in processing the data subject's personal information.

3.2 If a credit bureau does not collect information directly from the data subject and processes the information as an operator on behalf of a responsible party, it is not the credit bureau's obligation to ensure that the data subject is aware of the purpose of the collection but it must, in terms of the NCA, verify the originating source of the information and that personal information is lawfully collected.

3.3 If a credit bureau fails to ensure that a data subject is aware of the purpose of the collection of the information, who the responsible party is and to whom information may be transferred, the data subject cannot exercise its rights in terms of PoPIA and in particular, where it is entitled to do so, to object to the processing of his, her or its personal information.

A CREDIT BUREAU MUST:

- **If it collects information directly from a data subject, ensure that the data subject is aware of the specific, explicitly defined and lawful purpose of the collection of the personal information;**
- **If it does not collect information directly from a data subject, obtain written confirmation from the supplier of personal information, that:**
  - **where required, the prior consent of the data subject has been obtained; and**
  - **the data subject has received proper notification relating to the processing of the data as required in terms of Section 18(1) of PoPIA; alternatively**
  - **compliance with Section 18(1) is not necessary.**

Retention and restriction of records

14. (1) Subject to subsections (2) and (3), records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless—

(a) retention of the record is required or authorised by law;

(b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities;

(c) retention of the record is required by a contract between the parties thereto; or

(d) the data subject or a competent person where the data subject is a child has consented to the retention of the record.

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

(3) A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must—

(a) retain the record for such period as may be required or prescribed by law or a code of conduct; or

(b) if *there* is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

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

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

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

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

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

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

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

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

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

Other Applicable Legislation:

The NCA provides:

- *In Section 70(2)(d) that a registered credit bureau must retain consumer credit information for the prescribed period;*
- *In Section 70(2)(f) that a registered credit bureau must promptly expunge from its records consumer credit information that may not be entered into record or it is required to remove from its records;*

The NCA Regulation provides:

- *In Section 17 the retention periods for credit bureau information.*

3.4 The provisions of the NCA and those of PoPIA with regard to the retention of records are consistent.

3.5 PoPIA requires that personal information must not be retained for any longer than it is necessary but this is subject to the retention of the information as required by law.

3.6 As has previously been pointed out in this Code of Conduct, the NCA does not address the de-identification of information, nor does it address retention of information for historical, statistical or research purposes, both of which are referred to in PoPIA and are important considerations in establishing retention and destruction policies.

3.7 PoPIA requires that after a responsible party is no longer authorised to retain records it must destroy or delete the records in a manner that prevents its reconstruction in an intelligible form.

3.8 The de-identification of information requires the deletion of any information that allows for the identification of a data subject, its manipulation by a reasonably foreseeable method to identify the data subject or the linking of the information by a reasonably foreseeable method to other information that can identify the data subject.

3.9 In addition to the de-identification of personal information, in terms of the NCA the NCR may require records to be expunged. Expunge in its usual context means obliterate and remove completely. As consumer credit information is a class of personal information, the de-identification of information is sufficient to meet the requirements of the expunging of information and allow for the retention of de-identified information for historical, statistical or research purposes.

A CREDIT BUREAU MUST:

- **Retain personal information securely for the period authorised by law;**
- **Develop and maintain a Record Retention Policy that specifies the periods for retention of records, the security measures applied to records that are no longer displayed or used for purposes of credit scoring or credit assessment, and the destruction or de-identification of records containing personal information;**
- **Publish its Record Retention Policy on its website; and**
- **As soon as reasonably practicable after its retention is no longer necessary, destroy or de-identify the personal information.**

4. CONDITION 4: FURTHER PROCESSING LIMITATION

Further processing to be compatible with purpose of collection

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

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

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

(b) the nature of the information concerned;

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

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

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

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

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

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

(c) further processing is necessary—

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

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

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

(iv) in the interests of national security;

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

(i) public health or public safety; or

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

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

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

Other Applicable Legislation:

The NCA stipulates:

- *In section 3 the general purposes of the Act which, among other things, is to promote responsibility in the credit market by encouraging responsible borrowing by consumers and discouraging the reckless granting of credit by credit providers; Further, to improve consumer credit information and reporting;*
- *In Section 70 the nature of the information that may be processed and the actions of credit bureaux in achieving the purposes of the Act.*

The NCA Regulations prescribes:

- *In Sections 17 the retention periods for credit bureau information;*
- *In Section 18 the criteria governing the maintenance and retention of consumer credit information by a credit bureau; and*
- *In Section 19 the criteria governing the submission of consumer credit information to credit bureaux.*

4.1 The NCA and the NCA Regulations provide clear definition of the purpose of the parameters within which consumer credit information must be processed.

4.2 If any information is to be processed outside of the normal course of processing of the information by credit bureaux as stipulated in the NCA and prescribed in the NCA Regulations, this processing must be assessed by reference to the guidelines afforded by Sections 15(2) and (3) of PoPIA. This will assist in establishing whether the processing contemplated is compatible with the purpose for which the information was collected.

A CREDIT BUREAU MUST:

- **Establish reasonable commercial measures aimed at ensuring that personal information processed by it is processed for the purposes defined in the NCA and prescribed in the NCA Regulations;**
- **Not permit the further processing of information for a purpose incompatible with the purposes stipulated in the NCA and prescribed in the NCA Regulations.**

5. CONDITION 5: INFORMATION QUALITY

Quality of Information

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

(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.

Other Applicable Legislation:

The NCA stipulates:

- *In Sections 3(f) as one of its purposes, the improvement of consumer credit information and reporting;*
- *In Section 70(2) that a registered credit bureau must:*
  - *take reasonable steps to verify the accuracy of any consumer credit information reported to it;*
  - *not knowingly or negligently provide a report to any person containing inaccurate information.*
- *In Section 70(3) that in addition to consumer credit information as defined, a credit bureau may only receive, compile and report prescribed information from sources that are prescribed.*

The NCA Regulations prescribe:

- *In Section 19(3) that all sources of information must take reasonable steps to ensure that the information reported to a credit bureau is accurate, up to date, relevant, complete, valid and not duplicated.*

5.2 Critical to the advancement of the general purposes of the NCA to encourage responsible borrowing and discourage the reckless granting of credit is accurate consumer credit information. The requirement of ensuring information quality stipulated in PoPIA and the NCA are aimed at the same purpose of ensuring that the information which may affect decisions taken about a person is accurate. Unless the information is accurate it may result in decisions that unfairly prejudice that person.

5.3 In establishing an Information Security Management System as contemplated in Condition 7, in broad outline the aims are to ensure the confidentiality, integrity (information quality) and availability of information. The credit bureau's information security should promote the preservation of information quality as contemplated by both PoPIA and the NCA.

A CREDIT BUREAU MUST:

- **Establish measures to ensure the regular review of the quality of the information processed by the credit bureau;**
- **Establish measures to address and remedy instances where the quality of the personal information processed by it is found to be deficient and to as soon as reasonably practicable remedy the deficiency and correct personal information;**
- **Take all commercially reasonable measures, including, where appropriate, the conclusion of written agreements to obtain assurance from sources of information that the personal information provided to the credit bureau is accurate, up to date, relevant, complete, valid and not duplicated.**

6. CONDITION 6: OPENNESS

Documentation

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

Note: Section 14 of the Promotion of Access to Information Act applies to public bodies and as credit bureaux are by definition private bodies in terms of that Act, Section 14 is not applicable and only section 51 is applicable.

Other Applicable Legislation:

The Promotion of Access to Information Act, 2 of 2000:

- *In Section 51 provides:*

"51 Manual

(1) Within six months after the commencement of this section or the coming into existence of the private body concerned the head of a private body must compile a manual containing-

(a) the postal and street address, phone and fax number and, if available, electronic mail address of the head of the body;

(b) a description of the guide referred to in section 10, if available, and how to obtain access to it;

(c) the latest notice in terms of section 52 (2), if any, regarding the categories of record of the body which are available without a person having to request access in terms of this Act;

(d) a description of the records of the body which are available in accordance with any other legislation;

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

(f) such other information as may be prescribed.

(2) The head of a private body must on a regular basis update the manual referred to in subsection (1).

(3) Each manual must be made available as prescribed.

(4) For security, administrative or financial reasons, the Minister may, on request or of his or her own accord, by notice in the Gazette, exempt any private body or category of private bodies from any provision of this section for such period as the Minister thinks fit."

6.2 A fundamental purpose of PoPIA is to allow the data subject access to and knowledge of his or her personal information that is being processed by either of, or both responsible parties and operators. Even if the data subject has knowledge through collection of the information directly from him or her or notification as required in Section 18 of PoPIA, if the information indicating how the personal information is being processed is not available to the data subject he or she may be prevented from exercising the right to require amendment of inaccurate personal information or object to the processing of personal information, as stipulated in PoPIA.

6.3 The processing of personal information by a credit bureau is well regulated and credit bureaux should have policies, procedures and records relating to the processing of personal information that are properly documented and readily available to demonstrate how personal information is processed by them.

A CREDIT BUREAU MUST:

- **Ensure that written records (maintained electronically or physically) are available in terms of the NCA;**
- **Provide the details of records that are automatically available to data subjects or the data subject's duly authorised representative;**
- **Categorise and publish in a manual as contemplated in PAIA records that are automatically available without requesting access as contemplated in PAIA;**
- **Specify to whom records are automatically available in terms of both PoPIA and Section 18(4) of the NCA Regulations;**
- **Stipulate any conditions which may apply to the supply of the records to any person who may be entitled thereto;**
- **Before providing a record to any person including the data subject, or the data subject's duly authorised representative, identify the person (and if the person is a representative, verify the representative's authority) and confirm the purpose for which the record is required.**

Notification to data subject when collecting personal information

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

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

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

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

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

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

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

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

(h) any further information such as the—

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

(ii) nature or category of the information;

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

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

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

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

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

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

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

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

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

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

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

(c) non-compliance is necessary—

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

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

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

(iv) in the interests of national security;

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

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

(f) the information will—

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

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

Other Applicable Legislation:

The NCA does not have provisions which expressly correlate to Section 18 of PoPIA. However, the right to access and challenge credit records and information, which is stipulated in Section 72 of the NCA and which is more fully dealt with later in this Code of Conduct under Data Subject Participation, implies, in providing the right of access, that a consumer should be provided with knowledge of the who, how and what of the processing of this information.

6.6 To enable data subjects to exercise their rights relating to the processing of their information a critical prerequisite is knowledge of the who, how and what relating to their personal information. Without this knowledge the data subject is deprived of the right to object to the processing of their personal information, prevent direct marketing, establish where automated decision-making may adversely affect them, and correct inaccurate personal information.

6.7 Section 18(1) stipulates that it is the responsible party, which may not always be the credit bureau, that must take appropriate steps to notify data subjects. Nonetheless, as the NCA affords consumers the right to inspect any credit bureau or national credit register and to challenge the accuracy of information concerning the person, credit bureaux should take all reasonably practicable steps to ensure that the notification provisions stipulated in PoPIA facilitating the right to access have been fulfilled.

6.8 It is not the duty of the credit bureau to confirm whether the Data provider has complied with its obligations to notify the data subject of the purpose and manner of the processing of the data subject's personal information to enable a credit assessment. It is the duty of the credit bureau to take reasonable steps to verify the accuracy of consumer credit information reported to it.

6.9 If the accuracy of personal information is contested by a data subject the credit bureau must comply with the provisions of Section 72(3) to (6) of the NCA, in addition to the provision of access to personal information and the correction of personal information as contemplated in Sections 23 and 24 of PoPIA.

A CREDIT BUREAU MUST:

- **Publish on its website in a manual required in terms of PAIA:**
  - **the details of sources from which information may be collected;**
  - **the purpose of the collection of the information;**
  - **whether the supply of the information by the data subject is voluntary or mandatory;**
  - **that the information processed by credit bureaux is subject to the NCA; and**
  - **where applicable, details of cross border transfers of information.**
- **Publish on its website that, to the extent that the information processed by the credit bureaux is consumer credit information as defined in the NCA, its processing is subject to the provisions of the NCA, the NCA Regulations and rulings of the Credit Regulator;**
- **Publish on its website that the data subject has a right to access information, rectify incorrect information and object to the processing of personal information not subject to processing in terms of the NCA;**
- **Publish on its website that the data subject may lodge a complaint with the Information Regulator and/or the Credit Regulator as may be applicable, and provide contact details of both the Information Regulator and the Credit Regulator.**

While in terms of PoPIA, a credit bureau is obliged to obtain written assurance from the persons supplying the personal information to the credit bureau that that person has addressed a notification to the data subject, they are practically unable to obtain this assurance as Credit and Data providers who provide consumer credit information to credit bureaux are obliged by law to submit this information to credit bureaux without the consent of the consumer. Credit bureaux will accordingly be seeking an exemption to the provisions of this section from the Information Regulator.

7. CONDITION 7: SECURITY SAFEGUARDS

Security measures on integrity of personal information

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

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

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

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

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

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

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

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

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

Other Applicable Legislation:

The NCA stipulates:

- *In Section 3(f) as one of the purposes of the Act the improving of consumer credit information and reporting;*
- *In Section 68 that confidential information, being personal information that belongs to a person and is not generally available to or known by others, must be protected and its confidentiality safeguarded;*
- *In Section 70(2)(c) and (e) that a credit bureau must employ reasonable steps to verify the accuracy of information and maintain its records of consumer credit information in a manner that satisfies the prescribed standards;*
- *In Section 71 and 71A that a credit bureau is obliged in certain circumstances to remove and not report on certain categories of information which may adversely affect a consumer.*

The NCA Regulations prescribe:

- *In Section 18(1):*

"18(1) Records of consumer credit information must be maintained in accordance with the following standards …

(b) be collected, processed and distributed in a manner that ensures the records remain confidential and secure;

(c) be protected against accidental, unlawful destruction and unlawful intrusion;

(d) be protected against loss or wrongful alteration, and

(e) be protected against unauthorised disclosure or access by any authorised person."

- *That a credit bureau must take all reasonable steps to ensure that all records are kept up to date.*

7.1 The provisions of PoPIA are very similar in wording and materially identical in principle to those established in the NCA and the NCA Regulations. PoPIA expressly states that the responsible party must have regard to generally accepted information security practices and procedures. While this is absent from the NCA Regulations it can be implied because the discipline of information security is well documented and without adherence to generally accepted information security practices and procedures it would not be possible for a credit bureau to fulfil its obligations in terms of the NCA and NCA Regulations.

7.2 To comply with the Security Safeguards stipulated in PoPIA a credit bureau must establish and maintain an Information Security Management System ("ISMS") as required in generally accepted information security practice. An ISMS is part of an overall management system, based on a business risk approach, aimed at implementation, operation, monitoring, review and improvement of information security within an organisation.

7.3 An ISMS includes establishing an appropriate organisational infrastructure, developing policies (supported by procedures and standards) appropriate to the organisation, planning information security activities and assigning responsibilities as well as appropriate resources to the management of information security. It addresses information and communications technologies employed by the organisation in processing information, the procedures governing the appropriate use of the information and communications technologies and the training of all users of the information and communications technologies in the procedures governing their use.

7.4 The ISMS should provide reasonable assurance that the confidentiality, integrity and availability of information is maintained throughout the period from creation or receipt of the information to its eventual destruction by the organisation.

7.5 In establishing an ISMS an organisation must consider whether the information security control measures are appropriate to its operation. It must adopt control measures that are appropriate and should it exclude generally accepted control measures, in writing, justify the exclusion of these control measures.

A CREDIT BUREAU MUST:

- **Establish and maintain an ISMS that is appropriate to the management of the information processed by it, incorporating the appropriate security safeguards aimed at preventing the loss of, damage to or unauthorised destruction of personal information and the unlawful access to or processing of personal information;**
- **Determine the scope of the ISMS having regard to generally accepted information security practices and procedures, the practices employed in the processing of information in the credit industry, the law governing the processing of consumer credit information, and codes of conduct and standard operating procedures that regulate the processing of information in the credit industry.**

Information processed by operator or person acting under authority

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

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

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

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

Other Applicable Legislation:

The provisions of the NCA and the NCA Regulations referred to above apply in this instance.

7.6 In any circumstance that a credit bureau acts as an operator as defined in PoPIA, it may only process personal information with the knowledge and authorisation of the responsible party. Further, it is obliged to maintain the confidentiality of personal information processed by it and not to disclose it unless required by law or in the performance of its duties as a credit bureau.

A CREDIT BUREAU MUST:

- **In establishing an ISMS, take into account its responsibilities, as either/or both a responsible party or an operator, to maintain the confidentiality of personal information processed by it;**
- **If necessary, include the protections contained in Section 20 of PoPIA in written contracts to be concluded between responsible parties and operators in terms of Section 21 of PoPIA.**

Security measures regarding information processed by operator

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

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

Other Applicable Legislation:

There is no equivalent provision in the NCA, providing for a written contract between parties or the notification requirement in the event of a reasonable suspicion of the compromise of personal information.

The provisions of the NCA in Sections 3(f), 68, 70(2)(c), 21 and 71(A), as well as the NCA Regulations prescribed in Section 18(1) must be taken account of in considering written contracts to be concluded in terms of Section 21(1) of PoPIA.

7.7 Whether the credit bureau acts as a responsible party or an operator it must establish and maintain an ISMS.

7.8 Where the credit bureau is a responsible party it must conclude a written contract with all operators that process personal information under its mandate or in terms of a contract.

A CREDIT BUREAU MUST:

- **Where it acts as a responsible party conclude an agreement with an operator governing the security safeguards that must be established and maintained by the operator; and**
- **Include in the written contract provisions requiring that immediately the operator has reasonable grounds to believe that personal information of a data subject has been accessed or acquired by an unauthorised person, it notifies the credit bureau.**

Notification of security compromises

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

(a) the Regulator; and

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

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

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

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

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

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

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

(d) published in the news media; or

(e) as may be directed by the Regulator.

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

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

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

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

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

(6) The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

Other Applicable Legislation:

Neither the NCA nor NCA Regulations address notification of consumers relating to information security compromises.

7.9 It is accepted globally that data subjects have the right to know if the security of their personal information has been compromised. It is the data subject who is best placed to protect him or herself against the abuse of their personal information but unless the data subject has knowledge of the compromise they are deprived of this right.

7.10 Credit information is by its nature valuable and is typically regarded as sensitive. This is illustrated by the fact that in Chapter 11 of PoPIA dealing with Offences, Penalties and Administrative Fines unlawful acts by responsible parties and third parties in connection with "account numbers" receive special attention.

A CREDIT BUREAUX MUST:

- **Establish appropriate mechanisms to immediate notify the Regulator when reasonable grounds exist to believe that personal information of a data subject has been compromised;**
- **Unless instructed to the contrary by the Regulator, as soon as reasonably possible, notify the data subject of its knowledge or suspicion that the data subject's personal information has been accessed or acquired by an unauthorised person.**

8. CONDITION 8 : DATA SUBJECT PARTICIPATION

Access to personal information

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

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

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

(i) within a reasonable time;

(ii) at a prescribed fee, if any;

(iii) in a reasonable manner and format; and

(iv) in a form that is generally understandable.

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

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

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

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

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

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

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

Note: Credit bureaux are prohibited from processing health records and therefore the provisions of Section 61 of the Promotion of Access to Information Act is not applicable to credit bureaux.

Other Applicable Legislation:

The NCA stipulates:

- *In Section 72(1)(a) and (b):*

"72. (1) Every person has a right to-

(a) be advised by a credit provider within the prescribed time before any prescribed adverse information concerning the person is reported by it to a credit bureau, and to receive a copy of that information upon request;

(b) inspect any credit bureau, or national credit register, file or information concerning that person-

(i) without charge (aa) as of right once within any period of twelve months;

(bb) if so ordered by a court or the Tribunal; and

(cc) once within a reasonable period after successfully challenging any information in terms of this section, for the purpose of verifying whether that information has been corrected; and

(ii) at any other time, upon payment of the inspection fee of the credit bureau or national credit register, if any;"

The NCA Regulations:

- *In Section 18(1)(c) prohibits the records of a credit bureau containing medical status or history.*

8.1 In fulfilment of obligations stipulated in the NCA, credit bureaux have established procedures to advise consumers of adverse information and allow inspection of information concerning the consumer. Procedures which properly address the consumer's right to access information should satisfy, with possible minor adjustments, the rights of access to personal information afforded the data subject in terms of PoPIA.

8.2 If a credit bureau has not established appropriate procedures as contemplated in the NCA it must do so and ensure that these procedures accommodate the requirements of PoPIA.

A CREDIT BUREAU MUST:

- **Establish a process allowing the data subject access to personal information (consumer credit information);**
- **In response to any request for information, advise the data subject of his or her right to request the correction of inaccurate information; and**
- **If the credit bureau decides not to comply with the request for the correction of information by the data subject and the information is consumer credit information, when the credit bureau advises the data subject of its decision, it must also advise the data subject that he/she/it may refer a complaint to the NCR in terms of Section 136 of the NCA.**

Correction of personal information

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

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

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

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

(a) correct the information;

(b) destroy or delete the information;

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

(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

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

Other Applicable Legislation:

The NCA stipulates:

- *In Section 72(1)(c) and (d):*

  "72 (1) Every person has a right to- …

  (c) challenge the accuracy of any information concerning that person-

  (i) that is the subject of a proposed report contemplated in paragraph (a); or

  (ii) that is held by the credit bureau or national credit register, as the case may be, and require the credit bureau or National Credit Regulator, as the case may be, to investigate the accuracy of any challenged information, without charge to the consumer; and

  (d) be compensated by any person who reported incorrect information to a registered credit bureau or to the National Credit Register for the cost of correcting that information."

- *In Section 72(3):*

  "72 (3) If a person has challenged the accuracy of information proposed to be reported to a credit bureau or to the national credit register, or held by a credit bureau or the national credit register, the credit provider, credit bureau or national credit register, as the case may be, must take reasonable steps to seek evidence in support of the challenged information, and within the prescribed time after the filing of the challenge must-

  (a) provide a copy of any such credible evidence to the person who filed the challenge; or

  (b) remove the information, and all record of it, from its files, if it is unable to find credible evidence in support of the information, subject to subsection (6)."

8.3 In fulfilling their obligations in terms of the NCA, credit bureaux have established procedures for administering requests to correct information and the verification of the information that a consumer may request be corrected.

8.4 To the extent that a credit bureau has, in compliance with PAIA, published a manual setting out procedures addressing the manner of access to information, it will largely have complied with the provisions of Section 23 of PoPIA.

A CREDIT BUREAU MUST:

- **Establish appropriate mechanisms to deal with requests by data subjects to correct, delete or destroy inaccurate information;**
- **Establish procedures to notify the data subject of actions taken resulting from the data subject's request.**

9. PROCESSING OF SPECIAL PERSONAL INFORMATION

Prohibition on processing of special personal information

26. A responsible party may, subject to section 27, not process personal information concerning—

    (a) the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or

    (b) the criminal behaviour of a data subject to the extent that such information relates to—

        (i) the alleged commission by a data subject of any offence; or

        (ii) any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

Other Applicable Legislation:

The NCA Regulation stipulates:

- *In Section 18(3) that:*

"18 (3) Consumer credit information relating to the following subjects may not be contained on the records of the credit bureau:

(a) race;

(b) political affiliation;

(c) medical status or history;

(d) religion or thought, belief or opinion;

(e) sexual orientation, except to the extent that such information is self-evident from the record of the consumer's marital status and list of family members; and

(f) membership of a trade union, except to the extent that such information is self-evident from the record of the consumer's employment information."

9.1 Credit bureaux are expressly prohibited from processing the information contained in Section 18(3) of the NCA Regulations. These correlate closely to the provisions of Section 26(a) of PoPIA.

9.2 Section 26 further prohibits the processing of personal information relating to criminal behaviour, in respect of which a data subject has not yet been found guilty of an offence. This is not directly addressed in the NCA or NCA Regulations but credit bureaux do not process information of this nature.

9.3 In view of the fact that the processing of this information by a credit bureau is prohibited, the provisions governing the authorisation of the processing of this information in PoPIA are redundant.

A CREDIT BUREAU MUST:

A credit bureau must not process special personal information comprising of the information stipulated in Regulation 18(3) of the National Credit Act, and must not process other Special personal information unless the applicable provisions of s27 of PoPIA have been met.

10. PROCESSING OF PERSONAL INFORMATION OF CHILDREN

Prohibition on processing personal information of children

34. A responsible party may, subject to section 35, not process personal information concerning a child.

General authorisation concerning personal information of children

35. (1) The prohibition on processing personal information of children, as referred to in section 34, does not apply if the processing is—

(a) carried out with the prior consent of a competent person;

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

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

(d) for historical, statistical or research purposes to the extent that—

(i) the purpose serves a public interest and the processing is necessary for the purpose concerned; or

(ii) it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; or

(e) of personal information which has deliberately been made public by the child with the consent of a competent person.

(2) The Regulator may, notwithstanding the prohibition referred to in section 34, but subject to subsection (3), upon application by a responsible party and by notice in the Gazette, authorise a responsible party to process the personal information of children if the processing is in the public interest and appropriate safeguards have been put in place to protect the personal information of the child.

(3) The Regulator may impose reasonable conditions in respect of any authorisation granted under subsection (2), including conditions with regard to how a responsible party must—

(a) upon request of a competent person provide a reasonable means for that person to—

(i) review the personal information processed; and

(ii) refuse to permit its further processing;

(b) provide notice—

(i) regarding the nature of the personal information of children that is processed;

(ii) how such information is processed; and

(iii) regarding any further processing practices;

(c) refrain from any action that is intended to encourage or persuade a child to disclose more personal information about him- or herself than is reasonably necessary given the purpose for which it is intended; and

(d) establish and maintain reasonable procedures to protect the integrity and confidentiality of the personal information collected from children.

Other Applicable Legislation:

The NCA stipulates that credit agreements are unlawful if at the time that the agreement was made the consumer was an unemancipated minor unassisted by a guardian, unless the consumer or person acting on behalf of the consumer directly or indirectly, by an act of omission, induced the credit provider believe that the consumer had legal capacity to contract.

10.1 The National Credit Act is silent on the extension of credit to a child. In terms of PoPIA a child is defined as a natural person under the age of 18 years who is not legally competent. In those instances where a person under the age of 18 is no longer regarded as a child by virtue of emancipation or marriage, this provision would not apply.

10.2 It is competent for a child to open a banking account and the provision of credit to a child, duly assisted by a competent person (which is defined as anybody who is legally competent to consent to any action or decision being taken in respect of a matter concerning a child), may lead to the processing of consumer credit information by a credit bureaux.

A CREDIT BUREAU MUST:

- **If it processes a child's information obtain the prior consent of a competent person;**
- **Where a child's information is provided by a data supplier or data user, obtain written assurance that the prior consent of a competent person has been obtained;**
- **In all other instances ensure that a child's information is deleted as soon as reasonably possible after its receipt or its processing is no longer necessary for the purposes of the credit bureau performing is function.**

PART C – INFORMATION OFFICER, DIRECT MARKETING AND TRANSBORDER INFORMATION FLOWS

1. INFORMATION OFFICER

Duties and responsibilities of Information Officer

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

(a) the encouragement of compliance, by the body, with the conditions for the lawful processing of personal information;

(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;

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

(e) as may be prescribed.

(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 officers

56. 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 officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of this Act; and

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

Other Applicable Legislation:

The Promotion of Access to Information Act, 2 of 2002 ("PAIA"):

- *PAIA, in relation to a private body, defines the head of a juristic person as the chief executive officer or equivalent officer of the juristic person, or any person duly authorised by the Chief Executive Officer.*
- *In terms of PAIA it is the head or a person delegated by the head who acts on behalf of the organisation in fulfilling the organisation's obligations to provide access to records of the organisation;*
- *PAIA will, on the commencement of the Act, fall to be regulated by the Information Regulator appointed in terms of PoPIA.*

The NCA has no equivalent provisions.

1.1 An Information Officer is defined in relation to a private body, which is a juristic person, as either the Chief Executive (or equivalent) Officer or the person duly authorised by the Chief Executive (or equivalent) Officer.

1.2 In the case of credit bureaux unless the Chief Executive (or equivalent) Officer has appointed an Information Officer, the Chief Executive (or equivalent) Officer will be deemed to be the Information Officer.

1.3 PoPIA also stipulates that information officers must take up their duties only after the responsible party has registered them with the Regulator.

A CREDIT BUREAU MUST:

- **Provide appropriate training to allow the Information Officer to fulfil his/her statutory duties and organisational responsibilities; and**
- **Register the Information Officer/s that may be appointed by the credit bureau with the Information Regulator in a manner that may be prescribed by the Regulator as soon as this may become possible.**

2. DIRECT MARKETING BY MEANS OF UNSOLICITED ELECTRONIC COMMUNICATION AND AUTOMATED DECISION-MAKING

Direct marketing by means of unsolicited electronic communications

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

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

(b) is, subject to subsection (3), a customer of the responsible party.

(2) (a) A responsible party may approach a data subject—

(i) whose consent is required in terms of subsection (1)(a); and

(ii) who has not previously withheld such consent, only once in order to request the consent of that data subject.

(b) The data subject's consent must be requested in the prescribed manner and form.

(3) 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.

(4) 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.

(5) ''Automatic calling machine'', for purposes of subsection (1), means a machine that is able to do automated calls without human intervention.

Other Applicable Legislation:

NCA:

The NCA is silent as to direct marketing as it may affect credit bureaux. However, credit providers using information provided by credit bureaux will be subject to the provisions of PoPIA addressing Direct Marketing by way of Electronic Communications.

The Consumer Protection Act, 68 of 2008 ("CPA"):

The CPA deals relatively extensively with the right to fair and responsible marketing. This relates to all marketing of whatever nature and is not confined, as is the case with PoPIA, to direct marketing using electronic communications.

The CPA deals with direct marketing to consumers in Section 32. This stipulates that where, as a result of direct marketing, a transaction is concluded for goods and services the consumer must be informed of the right to rescind the agreement. Further, that if any goods are left with the consumer without payment being made, the goods are to be considered unsolicited goods.

2.1 The principles governing direct marketing by means of unsolicited electronic communications are straightforward. There is no restriction on direct marketing by electronic communication to existing customers, provided that the customer is afforded the opportunity of opting out of further communications with the responsible party.

2.2 Where the data subject is not a customer, consent to the processing of personal information for the purposes of direct marketing (opt in) is required. The responsible party is entitled to approach the data subject for consent to direct marketing in electronic communications unless such consent has previously been withheld. If the person approached does not expressly agree to receipt of further electronic communications (opt in), any further communications to that person will be unlawful.

2.3 In terms of the NCA the purpose of the processing of confidential information relates expressly to the provision of credit. If this information is used for another purpose such as direct marketing, this would be in breach of the Further Processing Limitations and unlawful.

A CREDIT BUREAU MUST:

- **Conclude written agreements with persons to whom personal information is provided that personal information, the purpose of which is to facilitate the grant of credit, will not be used by the receiver of the information, for the purposes of direct marketing, unless it is lawful and permissible under PoPIA or any other applicable legislation.**

Automated decision making

71. (1) Subject to subsection (2), a data subject may not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.

(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 of conduct in which appropriate measures are specified for protecting the legitimate interests of data subjects.

(3) The appropriate measures, referred to in subsection (2)(a)(ii), must—

(a) provide an opportunity for a data subject to make representations about a decision referred to in subsection (1); and

(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).

Other Applicable Legislation:

The NCA is silent with regard to automated decision making.

2.4 The prohibition against automated decision making in the context of granting of credit does not directly affect credit bureaux, provided that a decision which may result in legal consequences for a data subject has been taken in connection with the conclusion or execution of a contract, and either:

2.4.1 the request of the data subject in terms of the contract has been met; or

2.4.2 appropriate measures are in place to protect the data subject's legitimate interests in so far as automated decision making is concerned.

2.5 The protection of the legitimate interests of a data subject in this Code of Conduct is stipulated in Section 60(4)(a)(ii).

2.6 In addition to the reference to the protection of legitimate interests of data subjects in Section 71(2)(b) of PoPIA, the issue of legitimate interests of a data subject is addressed elsewhere in PoPIA.

2.7 Section 11(1) (dealing with the justification for the processing of personal information) stipulates that processing of personal information is lawful if it is:

2.7.1 in (d) the legitimate interests of the data subject; and

2.7.2 in (f) the legitimate interests of the responsible party or of a third party to whom information is supplied.

2.8 Similarly, Section 12 of PoPIA (dealing with the collection of information directly from a data subject) provides that collection from another source is permissible if:

2.8.1 the collection would not prejudice the legitimate interest of the data subject; and

2.8.2 collection from another source is necessary to maintain the legitimate interests of the responsible party, or of a third party to whom the information is supplied.

2.9 In many instances the legitimate interests of both the data subject on the one hand or a responsible party or third party on the other, would coincide. However, this is not always the case and the necessity exists to balance the legitimate interests of the data subject with that of the responsible party or a third party.

2.10 In considering this balance it will always be necessary to take cognizance of the constitutional rights entrenched in the Bill of Rights of our Constitution. These rights are not absolute and any limitation to these rights have to be considered by taking into account the nature of the right, the important of the purpose of the limitation, the nature and extent of the limitation, the relation between the limitation and its purpose and whether there are less restrictive means of achieving the purpose.

2.11 In the context of the consideration of “legitimate interest” in respect of the right to credit the purpose of the NCA (to promote equity in the credit market by balancing the respective rights and responsibilities of Data providers and consumers), would also need to be taken into account.

2.12 Against this background where automated decision making is employed in the processing of personal information by credit bureaux, a responsible party must, in protecting the legitimate interests of the data subject:

2.12.1 notify the data subject in terms of Section 18(1) that the processing of personal information may be subject to automatic decision making;

2.12.2 provide to the data subject sufficient information about the underlying logic of the automated decision-making technologies and processes to enable the data subject to make representations relating to the decision automatically made;

2.12.3 allow the data subject a reasonable opportunity for him or her to make representations to the responsible party about the decision.

A CREDIT BUREAU MUST:

Adopt appropriate measures for purposes of protecting the legitimate interests of the data subject, having regard to the outcome of information provided by way of any automated score generated by a credit bureau.

3. TRANSBORDER INFORMATION FLOWS

Transfers of personal information outside Republic

72. (1) A responsible party in the Republic may not transfer personal information about a data subject to a third party who is in a foreign country unless—

(a) the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that—

(i) effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and

(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.

(2) For the purpose of this section—

(a) ''binding corporate rules'' means personal information processing policies, within a group of undertakings, which are adhered to by a responsible party or operator within that group of undertakings when transferring personal information to a responsible party or operator within that same group of undertakings in a foreign country; and

(b) ''group of undertakings'' means a controlling undertaking and its controlled undertakings.

Other Applicable Legislation:

Neither the NCA nor the NCA Regulations address the transfer of consumer credit information to a foreign country.

3.1 The purpose of prohibiting the transfer of personal information to a foreign country is straightforward. If the foreign country does not have adequate protection of personal information the possibility exists that the personal information (information knowing no borders) may be processed in a manner that violates the data subject's right to privacy, including the right to determine the use of his or her personal information.

3.2 It is a feature of data protection legislation globally that unless the equivalent protection is provided in the foreign country, the transfer of the personal information to that country is prohibited, alternatively allowed subject to the fulfilment of conditions aimed to promote the protection of the personal information, regardless of the fact that there may be insufficient or inadequate laws in doing so in the foreign country.

A CREDIT BUREAU MUST:

- **Not transfer personal information about a data subject to a third party who is in a foreign country unless it has complied with the provisions of Section 72 of PoPIA;**
- **If the data subject consents to the transfer of his or her personal information to a foreign country, prior to the transfer obtain the written consent of the data subject, which may be in the form that the Information Regulator may determine;**
- **Even where the written consent of the data subject has been obtained, if the foreign country does not have adequate law protecting the personal information that an agreement, which may be in the form that the Information Regulator may determine, has been concluded prior to the transfer of the personal information to the foreign country;**
- **If the credit bureau has been instructed by a responsible party in respect of which it acts as an operator to transfer personal information to a foreign country, obtain a written warranty from the responsible party that the transfer of the personal information to a foreign country is in compliance with Section 72 of PoPIA.**

PART D – ENFORCEMENT

1. INTERPRETATION OF POPIA AND THIS CODE OF CONDUCT

1.1 For the purposes of the interpretation of PoPIA and this Code of Conduct as well as the enforcement of PoPIA and this Code of Conduct "business days" shall mean all weekdays which are not proclaimed public holidays in the Republic of South Africa.

1.2 The CBA Executive Manager shall, for the purposes of this Part D of the Conduct of Conduct, include any person assigned by the Executive Manager to discharge the Executive Manager's stipulated duties.

Consumers or Data Subjects

1.3 If consumers (as defined in the NCA) or data subjects (as defined in PoPIA) wish to complain about the conduct of a CBA member arising from an interpretation by the member of the NCA, the Regulations, PoPIA or this Code of Conduct the consumer or data subject must refer the complaint to the NCR or the Information Regulator, as may be appropriate.

1.4 If a consumer or data subject is aggrieved with the actions of a CBA member on the grounds that they are contrary to this Code of Conduct, the complaint must be made to the NCR or Information Regulator, as may be appropriate.

Interpretation and disputes relating to the Code of Conduct

1.5 If a member of the CBA wishes to request an interpretation of the Code of Conduct, or a complaint against another member of the CBA relating to an alleged breach of the Code of Conduct, the member may address the request or complaint in writing to the Executive Manager of the CBA.

1.6 If the request or complaint cannot be resolved by the CBA Executive Manager it will be placed on the agenda for discussion at the next meeting of representatives of CBA members.

1.7 If, at the meeting of CBA members, a request or a complaint cannot be resolved by the representatives of the members attending the meeting, the CBA Executive Manager must refer the request or complaint to the CBA Executive Committee.

1.8 The CBA Executive Committee may, in its discretion:

1.8.1 Make a decision and communicate the decision to the members of the CBA by eMail to its nominated representatives; or

1.8.2 Refer the request or complaint to legal counsel for consideration and opinion; or

1.8.3 Recommend to the CBA member requesting the interpretation or making the complaint to, at the member's cost, obtain an opinion from legal counsel and provide this to the Executive Manager.

1.9 Once an advice or opinion has been obtained from legal counsel the Executive Manager will circulate this to the Executive Committee and members of the CBA with a view to resolving the request or complaint.

1.10 If any member of the CBA remains aggrieved by the advice or opinion from legal counsel, they may request the CBA Executive Manager to again refer the matter to the Executive Committee, which may, but is not obliged to, appoint an independent adjudicator to consider and determine the request or complaint.

1.11 Nothing in this Code of Conduct prevents any member of the CBA from obtaining an independent advice or opinion from legal counsel or a subject matter expert, as may be appropriate and providing this to the Executive Committee.

Independent adjudicator

1.12 The CBA Executive Committee, if it chooses to appoint an independent adjudicator, will appoint an adjudicator who meets the criteria stipulated under the heading “Qualifications and Criteria for Independent Adjudicators” provided for below.

Qualifications and criteria for independent adjudicators

1.13 To be eligible for appointment as an independent adjudicator of the CBA, and to continue to hold that office, a person must—

1.13.1 not be subject to any disqualification set out in 1.14 below;

1.13.2 not have any interests referred to in 1.15 below;

1.13.3 be a natural person and a citizen of South Africa, who is ordinarily resident in the Republic; and

1.13.4 have suitable qualifications and/or experience in economics, law, commerce, industry and consumer affairs.

1.14 A person is disqualified for the appointment as an independent adjudicator of the CBA if that person—

1.14.1 is an office-bearer of any political party, movement, organisation or body of a partisan political nature;

1.14.2 personally, or through a spouse, partner, immediate family member or associate—

1.14.2.1 has or acquires a direct or indirect interest (whether financial or otherwise) in a member of the CBA or the CBA itself; or

1.14.2.2 has or acquires an interest in a business or enterprise, which may conflict or interfere or perceive to conflict or interfere with the proper performance of the duties of an independent adjudicator of the CBA;

1.14.3 is an unrehabilitated insolvent or becomes insolvent and the insolvency results in the sequestration of that person's estate;

1.14.4 has been removed from a position of trust on grounds of misconduct involving fraud, misappropriation of money, or any dishonesty;

1.14.5 is subject to an order of a competent court holding that person to be mentally unfit or mentally disordered;

1.14.6 within the previous 10 (ten) years has been convicted in the Republic of South Africa or elsewhere of theft, fraud, forgery or uttering a forged document, perjury, an offence under the Prevention and Combating of Corrupt Activities Act, No. 12 of 2004, an offence under the Financial Intelligence Centre Act, No. 38 of 2001, or an offence involving dishonesty; or

1.14.7 has been convicted of any other offence.

1.15 For the purpose of 1.14.2 above, a financial interest does not include an indirect interest held in any fund or investment if the person contemplated in that subsection has no control over the investment decisions of that fund or investment.

1.16 If approved and appointed as an independent adjudicator, then such independent adjudicator must promptly inform the CBA Executive Manager in writing after acquiring an interest that is, or is likely to become, an interest contemplated in 1.14.2 above.

1.17 If, at any time, it appears to an independent adjudicator that a matter referred to him/her for adjudication concerns an interest referred to in 1.14.2, that independent adjudicator must—

1.17.1 immediately and fully disclose the nature of that interest to the CBA Executive Manager; and

1.17.2 withdraw from the matter as adjudicator.

1.18 An independent adjudicator must not –

1.18.1 engage in any activity that may undermine the integrity or reputation of the CBA or any of its members;

1.18.2 adjudicate or influence the proceedings in any matter before adjudication if that person has an interest—

1.18.2.1 contemplated in 1.14.2 above; or

1.18.2.2 that precludes that person from performing the functions of an independent adjudicator in a fair, unbiased and proper manner;

1.18.3 make private use of, or profit from, any confidential information obtained as a result of performing that person's functions as an independent adjudicator of the CBA; or

1.18.4 divulge any information referred to in 1.18.3 to any third party, except as required as part of that person's official functions as an independent adjudicator of the CBA.

1.19 The Executive Manager of the CBA will seek appropriately qualified persons to be appointed as independent adjudicators.

Appointment and powers of adjudicator

1.20 The CBA Executive Committee may appoint any one, or if it deems necessary, more than one of the independent adjudicators approved by the CBA Executive Committee to hear the complaint and adjudicate thereon.

1.21 The adjudicator must apply the principles stipulated in Section 44 of PoPIA in determining any decision which relates to the unlawful processing of personal information.

1.22 The adjudicator may in addition to information provided to him or her, call for further information or summon the complainant or representatives of a CBA member to provide oral evidence and, if the adjudicator deems appropriate, allow cross-examination of a witness.

1.23 On completion of his or her investigation the independent adjudicator must send a report containing its determination, together with reasons therefor, to the CBA Executive Manager and the CBA member.

1.24 If the CBA member is determined to be in breach of this Code the adjudicator may make or give any order, declaration or direction requiring that the CBA member takes any specific actions within a reasonably stipulated period of time, failing which any one or more of the sanctions available in the CBA's constitution may be imposed, and such determination shall, unless formally disputed, be final and binding upon the CBA member.

1.25 If any member of the CBA remains aggrieved by the decision the CBA member may refer the dispute to the Information Regulator in terms of Chapter 10 of PoPIA.

1.26 Nothing in this Part D shall in any way restrict or detract from the provisions of Chapter 10 of PoPIA.

Retention of information relating to disputes

1.27 The CBA Executive Manager must collect and securely retain information relating to requests and complaints as well as all records of proceedings and decisions that may be made relating to requests or complaints that are made in terms of this Code of Conduct.

1.28 The CBA Executive Manager must submit an annual report to the Regulator specifying the complaints, the nature of the complaints, the treatment of the treatment of the complaints and the determinations made by the CBA Executive Manager, the CBA panel or an independent adjudicator what occurred during the year following the provision of the annual report to the Regulator.

1.29 Nothing in this Part D shall in any way limit, restrict or detract from the provisions in Chapter 10 of PoPIA.

PART E – ADMINISTRATION OF CODE OF CONDUCT

1. COMPLIANCE WITH CHAPTER 7 OF POPIA

Issue of Code of Conduct

1.1 This Code of Conduct applies to credit bureaux registered in terms of Section 43 of the NCA that is a member (regardless of category of membership) of the CBA.

1.2 Credit bureaux who are members of the CBA have mandated the CBA to apply to the Information Regulator for the issue of this Code of Conduct.

1.3 The Code of Conduct incorporates the conditions for the lawful processing of personal information and provides functional equivalence of obligations set out in those conditions that are applicable to the conduct of credit bureaux as regulated by the NCA and as may be prescribed by the NCA Regulations.

Legitimate interests of data subjects

1.4 This Code of Conduct specifies appropriate measures for protecting the legitimate interests of data subjects with regard to "Automated Decision Making" in Part C.

Review

1.5 This Code of Conduct will be reviewed by the CBA within 1 (one) year of its coming into force in terms of Section 62(2) of PoPIA.

1.6 Further reviews of this Code of Conduct will be conducted annually by no later than the anniversary of the date of the coming into force of this Code of Conduct.

1.7 The review of this Code of Conduct may be accelerated:

1.7.1 if an earlier review is prescribed by the Regulator in writing addressed to the CBA Executive Manager; or

1.7.2 required in terms of a ruling made by the Regulator; or

1.7.3 if directed to do so by the Regulator in an Information Notice issued in terms of Section 90 or an Enforcement Notice issued in terms of Section 95 of PoPIA; or

1.7.4 if any court having jurisdiction over credit bureaux who is a member of the CBA directs that any provisions of this Code of Conduct are unlawful.

Amendment of the Code of Conduct

1.8 The CBA will revoke or make any amendments to the Code of Conduct as directed by the Regulator or mandated by its members, in compliance with Sections 60 to 63 of PoPIA.

Expiry

1.9 This Code of Conduct will continue to be of force and effect indefinitely, subject to the Regulator's direction as to the date of its expiry or termination by the CBA.

1.10 On the termination of this Code of Conduct all members of the CBA will remain subject to the provisions of PoPIA and any other applicable laws governing the processing of personal information.

Publication of Code of Conduct

1.11 From the date that the Code of Conduct comes into force the CBA will cause publication of the Code on its website and require that its members publish the Code on their websites.

1.12 The CBA will make copies of the Code available in hardcopy form to persons requesting a copy in that form.

Interpretation

1.13 The interpretation of PoPIA and of this Code of Conduct as they relate to the operation of credit bureaux may be made by the CBA Executive Manager. No interpretation made by the CBA Executive Manager shall be binding on the Information Regulator or detract from any of the powers of the Information Regulator stipulated in Chapter 10 of PoPIA.

Revision History

1.14 The CBA Executive Manager will ensure that a revision history of this Code of Conduct will be established and maintained.

1.15 The revision history must record the material aspects of any decisions or rulings made by the Regulator or by the CBA Executive Committee that cause amendments to be made to this Code of Conduct.

APPENDIX A

THE 8 CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION CONTAINED IN THE PROTECTION OF PERSONAL INFORMATION ACT, NO. 4 OF 2013 OF THE REPUBLIC OF SOUTH AFRICA

PROTECTION OF PERSONAL INFORMATION ACT 4 OF 2013

CHAPTER 3

CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

Part A

Processing of personal information in general

Condition 1
Accountability

Responsible party to ensure conditions for lawful processing

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

Condition 2
Processing limitation

Lawfulness of processing

9. Personal information must be processed—

(a) lawfully; and

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

Minimality

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

Consent, justification and objection

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

(a) the data subject or a competent person where the data subject is a child consents to the processing;

(b) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

(c) processing complies with an obligation imposed by law on the responsible party;

(d) processing protects a legitimate interest of the data subject;

(e) processing is necessary for the proper performance of a public law duty by a public body; or

(f) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

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

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

(3) A data subject may object, at any time, to the processing of personal information─

(a) in terms of subsection (1)(d) to (f), in the prescribed manner, on reasonable grounds relating to his, her or its particular situation, unless legislation provides for such processing; or

(b) for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications as referred to in section 69.

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

Collection directly from data subject

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

(2) It is not necessary to comply with subsection (1) if—

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

(b) the data subject or a competent person where the data subject is a child has consented to the collection of the information from another source;

(c) collection of the information from another source would not prejudice a legitimate interest of the data subject;

(d) collection of the information from another source is necessary—

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

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

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

(iv) in the interests of national security; or

(v) to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;

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

(f) compliance is not reasonably practicable in the circumstances of the particular case.

Condition 3
Purpose specification

Collection for specific purpose

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

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

Retention and restriction of records

14. (1) Subject to subsections (2) and (3), records of personal information must not be retained any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless—

(a) retention of the record is required or authorised by law;

(b) the responsible party reasonably requires the record for lawful purposes related to its functions or activities;

(c) retention of the record is required by a contract between the parties thereto; or

(d) the data subject or a competent person where the data subject is a child has consented to the retention of the record.

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

(3) A responsible party that has used a record of personal information of a data subject to make a decision about the data subject, must—

(a) retain the record for such period as may be required or prescribed by law or a code of conduct; or

(b) if there is no law or code of conduct prescribing a retention period, retain the record for a period which will afford the data subject a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

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

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

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

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

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

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

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

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

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

Condition 4
Further processing limitation

Further processing to be compatible with purpose of collection

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

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

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

(b) the nature of the information concerned;

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

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

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

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

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

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

(c) further processing is necessary—

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

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

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

(iv) in the interests of national security;

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

(i) public health or public safety; or

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

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

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

Condition 5
Information quality

Quality of information

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

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

Condition 6
Openness

Documentation

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

Notification to data subject when collecting personal information

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

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

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

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

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

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

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

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

(h) any further information such as the—

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

(ii) nature or category of the information;

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

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

(v) **[the]** right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator, which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the data subject to be reasonable.

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

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

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

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

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

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

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

(c) non-compliance is necessary—

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

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

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

(iv) in the interests of national security;

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

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

(f) the information will—

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

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

Condition 7
Security Safeguards

Security measures on integrity of personal information

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

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

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

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

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

(b) establish and maintain appropriate safeguards against the risks identified;
(c) regularly verify that the safeguards are effectively implemented; and
(d) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

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

Information processed by operator or person acting under authority

20. An operator or anyone processing personal information on behalf of a responsible party or an operator, must—
(a) process such information only with the knowledge or authorisation of the responsible party; and
(b) treat personal information which comes to their knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.

Security measures regarding information processed by operator

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

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

Notification of security compromises

22. (1) Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify—
(a) the Regulator; and
(b) subject to subsection (3), the data subject, unless the identity of such data subject cannot be established.

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

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

(4) The notification to a data subject referred to in subsection (1) must be in writing and communicated to the data subject in at least one of the following ways:
(a) Mailed to the data subject's last known physical or postal address;
(b) sent by e-mail to the data subject's last known e-mail address;
(c) placed in a prominent position on the website of the responsible party;
(d) published in the news media; or

(e) as may be directed by the Regulator.

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

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

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

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

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

(6) The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of personal information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the compromise.

Condition 8
Data subject participation

Access to personal information

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

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

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

(i) within a reasonable time;

(ii) at a prescribed fee, if any;

(iii) in a reasonable manner and format; and

(iv) in a form that is generally understandable.

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

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

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

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

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

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

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

Correction of personal information

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

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

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

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

(a) correct the information;

(b) destroy or delete the information;

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

(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

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