Government Gazette
Staatskoerant

REPUBLIC OF SOUTH AFRICA
REPUBLIEK VAN SUID AFRIKA

Vol. 688 7 October / Oktober 2022 No. 47257

PART 1 OF 4

ISSN 1682-5845

9 771682 584003 47257

DEPARTMENT OF JUSTICE AND CONSTITUTIONAL DEVELOPMENT

NO. 2601 **7 October 2022**

INFORMATION REGULATOR (SOUTH AFRICA)
Ensuring protection of your personal information and effective access to information

Address: 27 Stiemens Street, 4th Floor
JD House Building, Braamfontein,
Johannesburg, 2017
Tel: 010 023 5214
Fax: 0865003351
E-mail: POPIACompliance@inforegulator.org.za

27 SEPTEMBER 2022

NOTICE IN TERMS OF SECTION 62(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT NO 4 OF 2013 (POPIA) CODE OF CONDUCT: THE BANKING ASSOCIATION SOUTH AFRICA(BASA)

1. In terms of the provisions of section 62(1) of POPIA, the Information Regulator (Regulator) gives notice of issuing a code of conduct submitted by The Banking Association South Africa to the Regulator on 31 May 2022 that deals with how personal information will be processed in the credit sector.
2. On 24 June 2022, the Regulator gave notice upon receipt of the Code in terms of the provisions of section 61(2) of POPIA for submissions to be made on the code of conduct to be issued.
3. The purpose of the code of conduct is to-
   3.1. promote appropriate practices by members of BASA governing the processing of personal information in terms of POPIA;
   3.2. encourage the establishment of appropriate agreements between members of BASA and third parties, regulating the processing of personal information as required by POPIA and dictated by good business practice; and
   3.3. to establish procedures for members of BASA to be guided in their interpretation of principally POPIA, but also other laws or practices governing the processing of personal information, allowing for complaints against credit bureau to be considered and remedial action, where appropriate, to be taken.
4. The code of conduct governs-
   4.1. the processing of personal information (including consumer credit information) by credit bureau that are members of BASA in compliance with POPIA and The Banks Act, 94 of 1990;

4.2. where appropriate, agreements that may need to be concluded between members of BASA and third parties promoting, and to the extent possible ensuring that personal information is processed in compliance with POPIA; and

4.3. the enforcement by BASA of the provisions of the code of conduct,

5. The Regulator has considered the proposed code of conduct in terms of section 60 of POPIA, and herein provides notice that an application for the issuing of a BASA code has been successful and it is being issued in pursuance of section 62(1) as follows:

5.1. copies of the code are available for inspection free of charge and for purchase;

5.2. copies of it are available on the Regulator's website as long as the code remains in force;

5.3. The BASA code is binding on every class or classes of body, industry, profession or vocation referred to therein.

5.4. The Regulator may on its own initiative review the operation of an approved code within a five (5) year period or as and when deemed necessary.

5.5. The outcome of the review of a code may inform a decision by the Regulator to revoke an approved code.

6. A code of conduct issued under section 60 of POPIA will come into force on the 28th day after the date of its notification in the Gazette.

7. A copy of the code of conduct will be made available on the Regulator's website, alternatively, a request for a copy of the code may be made by addressing correspondence to email address: POPIACompliance@inforegulator.org.za

THE BANKING ASSOCIATION SOUTH AFRICA

Tel +27 11 645 6700
Fax +27 11 645 6800
P O Box 61674
Marshalltown 2107
www.banking.org.za

3rd Floor Building D
Sunnyside Office Park
32 Princess of Wales Terrace
Parktown 2193

CODE OF CONDUCT FOR THE PROCESSING OF PERSONAL INFORMATION BY THE BANKING INDUSTRY

1 INTRODUCTION AND SCOPE OF THE CODE

1.1 The Banking Association of South Africa ("**BASA**") is an industry association whose members are those banks licenced to operate in South Africa.

1.2 BASA advances the interests of the banking industry with its regulators, legislators, and stakeholders, with the objective of making banking sustainable, profitable, and better able to contribute to the social and economic development and transformation of South Africa.

1.3 The Information Regulator ("**Regulator**") has issued this Code in terms of chapter 7 of the Protection of Personal Information Act 4 of 2013 ("**POPIA**") after application was made by BASA, representing the member banks. A list of the member banks is available on BASA's website at www.banking.org.za.

1.4 The field of application of POPIA and its regulations would apply to this Code.

1.5 BASA and its members recognise the constitutional right to privacy and support the safeguarding of personal information when processed by a responsible party in accordance with the provisions of POPIA.

1.6 The Code is intended to outline and expand on the specific obligations of the members of BASA, i.e., the banks, as responsible parties, operators, or as joint responsible parties, when processing the personal information of data subjects and will not replace the provisions of POPIA.

1.7 In the event of a conflict between POPIA and this Code; POPIA would prevail.

1.8 Member banks may be part of a group of companies where other companies within the group also offer financial products and services and non-financial products and services. These financial and non-financial products and services may fall outside the scope of banking products and services and may for example include telecommunication, loyalty rewards, roadside assistance, insurance, shares and various other products and services. In these instances, member banks may act as an operator or as joint responsible party together with other entities within that group of companies and personal information may be processed where there are lawful grounds to do so. Whilst operating within a group of companies, member banks and other companies within their group of companies will always comply with all the obligations set out within the Code and with other applicable laws whenever offering any products and services.

1.9 If a member bank transfers personal information to a third party (which is a company within the aforementioned group of companies) in a foreign country, the member bank will ensure that binding corporate rules and / or inter group agreements, which would govern the conditions for the lawful processing of the personal information of data subject within the group is in place.

1.10 The Code applies to the various processing activities by member banks, which include:

1.10.1 Financial services related processing activities, which enables the provision of transactional, investment, lending and insurance products and services; including the provision of value-add products and services.

1.10.2 Employee related processing activities, which enables the provision of the member's human capital resources/employee management activities.

1.10.3 Supplier and business partner related processing activities, which includes but is not limited to the enablement of the member's procurement related activities.

1.11 The Code outlines specific processing practices which demonstrate how the conditions for the lawful processing of personal information will be applied by the member banks. The specific processing practices included in the Code are not intended to be an exhaustive list of all the processing activities undertaken by member banks.

1.12 The content of the Code is aligned to and compliant with the requirements of POPIA.

2 DEFINITIONS

2.1 The headings of the clauses in this Code are for the purpose of convenience and reference only and shall not be used in the interpretation, modification, or amplification of the terms of this Code or any clause hereof.

2.2 For purposes of this Code –

2.2.1 any one gender includes the other genders;

2.2.2 the singular includes the plural and vice versa;

2.2.3 references to "includes" or "including" are to be construed without limitation;

2.2.4 references to any statute include all subordinate legislation made thereunder and any amendment or re-enactment from time to time;

2.3 In this Code, the following expressions shall bear the meanings assigned to them below and related expressions bear corresponding meanings:

2.3.1 **"automated means"** for the purposes of this Code, means any equipment capable of operating automatically in response to instructions given for the purpose of processing information;

2.3.2 **"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;

2.3.3 **"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;

2.3.4 **"Code"** means this code of conduct issued in terms of Chapter 7 of POPIA;

2.3.5 **"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 (for example, a parent of the child or a legal guardian of the child);

2.3.6 **"data subject"/"you"/"your"** means the person to whom the personal information relates and for the purpose of this Code may, include but is not limited to, customers, prospective customers, past customers, suppliers, prospective suppliers, past suppliers, employees, prospective employees or past employees of member banks and the related parties to these persons;

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

2.3.7.1 identifies the data subject;

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

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

2.3.8 **"financial services"** has the same meaning ascribed to it in section 3(1) of the Financial Sector Regulation Act 9 of 2017;

2.3.9 **"group of companies"** has the same meaning ascribed to it in terms of section 1 of the Companies Act 71 of 2008;

2.3.10 **"group of undertakings"** means a controlling undertaking and its controlled undertakings;

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

2.3.12 **"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;

2.3.13 **"PAIA"** means the Promotion of Access to Information Act 2 of 2000;

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

2.3.15 **"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—

2.3.15.1 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;

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

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

2.3.15.4 the biometric information of the person;

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

2.3.15.6 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;

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

2.3.15.8 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;

2.3.16 **"POPIA"** means the Protection of Personal Information Act 4 of 2013;

2.3.17 **"prescribed"** means prescribed by POPIA or by this Code;

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

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

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

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

2.3.19 **"public body"** means-

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

2.3.19.2 any other functionary or institution when-

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

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

2.3.20 **"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;

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

2.3.22 **"responsible party"/"we"/"us"**, for purposes of this Code, a bank which is a member of BASA and which, alone or in conjunction with others (as joint responsible parties), determines the purpose of and means for processing personal information.

2.3.23 Any term used in this Code will carry the definition as allocated by POPIA and its regulations unless the contrary is indicated in this document.

A CONDITIONS FOR LAWFUL PROCESSING

3 ACCOUNTABILITY

3.1 We will ensure that the conditions for the lawful processing of personal information as set out in Chapter 3 of POPIA, 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.

3.2 The member banks, in adherence with the Banks Act 94 of 1990, have compliance functions; the operations of which are governed by compliance frameworks. The compliance frameworks consider the identification, management, monitoring and reporting of compliance risk. This includes, but is not limited to:

3.2.1 The identification of compliance risks entails the compilation of a regulatory risk universe applicable to a specific member bank. The member bank must include POPIA in its regulatory risk universe. Inherent and residual risks will be assigned to a regulatory requirement identified as being applicable to a business area within a member bank. The member banks must identify the inherent and residual risks of the regulatory requirements of POPIA.

3.2.2 The identified regulatory risks relating to POPIA must be managed by the member bank. The member bank may use a risk management plan. This plan will document the controls in place or to be developed by the member bank to adhere to the specific regulatory requirements in POPIA and to mitigate the risk of non-compliance with POPIA.

3.2.3 The compliance function of the member bank must monitor:

3.2.3.1 the adequacy of the controls to verify that they exist and that they mitigate the risk of non-compliance with POPIA; and

3.2.3.2 the effectiveness of the controls relevant to POPIA to verify that they are applied consistently by the member bank across a specific timeline.

3.2.4 In the event of any control gaps within the member bank, agreed actions will be documented to address any areas of non-compliance or inadequate controls as it relates to POPIA.

3.3 The Information Officer of each member bank will ensure that this Code forms an integral part of how compliance to POPIA is achieved.

3.4 Each member bank's governance frameworks support ethical and effective leadership, corporate citizenship, and sustainable organisational and societal outcomes.

4 PROCESSING LIMITATION

4.1 We will process personal information lawfully and in a reasonable manner that does not infringe your right to privacy, and only if, given the purpose for which it is processed, it is–

4.1.1 adequate (i.e., sufficient to properly fulfil our stated purpose);

4.1.2 relevant (i.e., the personal information has a rational link to that purpose); and

4.1.3 not excessive (i.e., ensuring we do not hold more personal information than we need for the stated purpose).

4.2 In addition, we will ensure that we have a lawful basis for processing that personal information, which may be one or more of the following –

4.2.1 your consent to the processing; or

> When we rely on consent to process your personal information, we will ensure that the consent is voluntary, specific, and an informed expression of will indicating your permission for the processing of personal information. Consent will therefore be given by a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of your agreement to the processing of your personal information. Such an affirmative act could be provided by a written statement, including by electronic means, or an oral statement, ticking a box when completing an online application, or another statement or conduct which clearly indicates your acceptance of the proposed processing of your personal information. For example, when you visit a website, you may be required to consent to the use of cookies on that website where those cookies identify you as the data subject. (Cookies are small pieces of data, stored in text files, that are stored on the device you use to access the website. The cookies are used to "remember" you and your preferences when you visit that website again).

4.2.2 the processing is necessary to carry out actions for the conclusion or performance of a contract to which you are a party; or

> Where you enter into an agreement with us or agree to the terms and conditions of a product or service, processing of your personal information will be necessary for the conclusion and performance of that agreement. This may include, but is not limited to, opening, managing and maintenance of the

account, obtaining a credit facility, subscribing you to a service, delivering the access device or card, concluding a supplier or employment contract, or managing complaints and queries.

4.2.3 the processing complies with an obligation imposed by law on us; or

The financial services industry is a highly regulated sector. Member banks are required to process personal information in compliance with financial laws and regulations as well as other applicable laws. Such laws may deal with -

(i) crime prevention, detection, and reporting of actual or suspected theft, fraud, money laundering, corruption, and other crimes;
(ii) market conduct, which provides for the conducting of market and behavioural research, including scoring and analysis to determine if a customer or potential customer qualifies for products, to determine a customer's or potential customer's credit or insurance risk, to ensure that the most appropriate products are provided to customers or potential customers and to develop and improve these products within the group of companies to which the member bank belongs;
(iii) credit, which requires conducting of affordability assessments, credit assessments and credit scoring, as well as the disclosure and collection of personal information from credit bureaux regarding a customer's or potential customer's credit history;
(iv) labour relations, and which impose certain obligations on member banks as employers;
(v) tax collection and reporting;
(vi) compliance and risk management which may include the management of compliance with legislative, regulatory, risk and compliance requirements which may also be prescribed in directives, codes of conduct and industry agreements;
(vii) protection for whistle-blowers. Banks as public companies are for example obliged to establish and maintain a system to receive disclosures confidentially, and act on them;
(viii) record-keeping obligations in accordance with applicable laws; and
(ix) complying with reporting and information requests from regulatory authorities, courts, tribunals or in terms of PAIA.

4.2.4 the processing protects your legitimate interest; or

Banks will process the personal information of its financial customers in order to design its financial products and services, including related models utilised for determining the advertising, distributions and provision of these financial products and services with due regard to protecting the interests of its customers or potential customers. The financial products and services will therefore meet the needs of the data subjects and the performance of the products and services will be designed to meet the expectation of the data subjects.

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

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

We will consider your rights when assessing our legitimate interests and in doing so ensure that the processing is necessary for our legitimate interest or the legitimate interest of a third party, unless there is a good reason to protect your personal information which overrides the legitimate interests we wish to rely on.

These legitimate interests may include (but is not limited to) –

(i) developing, implementing, monitoring, and improving business processes, policies, and systems, business risk mitigation;
(ii) managing business continuity and emergencies;

(iii) developing, testing, and improving products and services for customers and potential customers;

(iv) tailoring solutions which would include consideration of a customer's use of third-party products, goods, and services and in accordance with applicable laws, the marketing of appropriate solutions to the customer, including marketing on the member bank's own or other websites, mobile applications, and social media;

(v) responding to enquiries and communications including the recording of engagements in accordance with applicable laws and analysing the quality of the engagements with data subjects;

(vi) responding to complaints including analytics of complaints to understand trends and prevent future complaints;

(vii) enforcing and collecting on any agreement when a customer is in default or has breached the terms and conditions of the agreement, which includes tracing the customer and instituting legal proceedings against the customer. In such instances, we may verify the customer's details against third party data bases to determine the customer's most accurate contact details in order to enforce or collect on any agreement we may have with the customer;

(viii) processing payment instruments and payment instructions (such as a debit orders);

(ix) creating, manufacturing, and printing payment instruments and payment devices (such as a debit card);

(x) complying with codes of conduct and industry agreements;

(xi) detection, prevention and reporting of theft, fraud, money laundering, corruption, and other crimes. This may include the processing of special personal information in accordance with applicable laws, such as alleged criminal behaviour or the supply of false, misleading, or dishonest information when opening an account, or avoiding liability by way of deception. We will also monitor access to our buildings by using CCTV cameras and implementing access control;

(xii) in accordance with applicable laws, conducting market and behavioural research, including scoring and analysis to determine if a customer or potential customer qualifies for products, services, or to determine a customer's or potential customer's credit or insurance risk;

(xiii) statistical purposes, such as market segmentation or customer segmentation (that is placing customers in groups with similar customers based on their personal information);

(xiv) enabling customers to participate in customer rewards programmes which includes determining customer qualification for participation, rewards points, rewards level, and monitor customer buying behaviour with the group's rewards partners to allocate the correct points or inform customers of appropriate products or services they may be interested in, or to inform reward partners about a customer's purchasing behaviour;

(xv) for customer satisfaction surveys, promotional and other competitions;

(xvi) disclosing and obtaining personal information from credit bureaux regarding a customer's or potential customer's credit history;

(xvii) developing credit models and credit tools which are used to assess credit risk, the pricing for credit products, the suitability of credit products and assist with meeting various banking prudential obligations; and

(xviii) financing or risk management in relation to a commercial arrangement for our customers, involving an underlying transaction to which you are a party, such as import / export financing or receivables financing/factoring.

4.3 We will collect personal information directly from you or from someone authorised by you, unless -

4.3.1 the information is contained in or derived from a public record or has deliberately been made public by you;

We may collect your personal information when you have deliberately or someone on your behalf has made your personal information public by for example publishing it on social media, commenting on public forums (i.e., a web blog), or directing messages to us on social media sites.

We may also collect your personal information from public records which may include -

(i) the Companies Intellectual and Property Commission;
(ii) the National Credit Regulator;
(iii) published court records;
(iv) the Deeds Office established in terms of the Deeds Registries Act 47 of 1937; or
(v) the Masters' offices established in terms of the Administration of Estates Act 66 of 1965.

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

4.3.3 the collection of the information from another source would not prejudice your legitimate interest;

4.3.4 the collection of the information from another source is necessary -

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

4.3.4.2 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 34 of 1997;

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

4.3.4.4 in the interests of national security; or

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

4.3.4.6 compliance would prejudice a lawful purpose of the collection;

4.3.4.7 compliance is not reasonably practicable in the circumstances of the particular case;

We will also not collect information directly from a data subject in the following instances (which are not intended to be exhaustive) –

(i) if our customer is a third-party payment provider ("**TPPP**") as contemplated under section 7(c) of the National Payment System Act 78 of 1998 and we ask our customer to provide us with the details of the TPPP's clients on whose behalf the TPPP either collects payment or makes payment to;
(ii) if we ask a prospective customer to provide us with the details of his/her employer;
(iii) the representative of a company or other juristic person is authorised to provide us with the personal information of other directors, members, trustees, shareholders, sureties, partners, other authorised representatives or cessionaries;
(iv) the primary cardholder (i.e., the person in whose name a credit card has been issued and who is responsible to pay the credit card account) asks us to issue a card to a secondary cardholder and provides us with the personal information of that secondary cardholder (i.e. a person who is authorised to use the card but who is not responsible to pay the credit card account);
(v) we issue fleet cards to the employees of our customer who provides us with the personal information of those employees;
(vi) if we require the information for the complaint's management processes of the member banks;
(vii) if we process information in accordance with the Disaster Management Act 57 of 2002 where a national state of disaster has been declared; or

(viii) if we process the information to investigate alleged or suspected fraud.

5 PURPOSE SPECIFICATION

5.1 Personal information will be collected for a specific, explicitly defined, and lawful purpose related to a function or activities of the member banks. Refer to the member banks' privacy notices published on their websites where they provide explanations regarding the purposes for which a customers' personal information may be used.

5.2 ***Retention and restriction of records***

5.2.1 We will not retain records of personal information any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed, unless-

5.2.1.1 retention of the record is required or authorised by law;

We are required to retain your personal information in terms of (but not limited to) the following laws:

(i) the National Payment System Act 78 of 1998 requires us to retain all records obtained by us during the course of the operation and administration of a payment for a period of 5 (five) years from the date of each particular record;

(ii) the National Credit Act 34 of 2005 requires us to keep records for 3 (three) years from the date of termination of a credit agreement; or in the case of an application for credit that is refused or not granted for any reason, from the date of receipt of the application;

(iii) the Financial Intelligence Centre Act 38 of 2001 requires us to keep records which relate to-

a. the establishment of a business relationship, for at least 5 (five) years from the date on which the business relationship is terminated;

b. a single transaction which is concluded, for at least 5 (five) years from the date on which that transaction is concluded; and

c. a transaction or activity which gave rise to a report contemplated in section 29 (i.e., reports relating to suspicious and unlawful activities), for at least 5 (five years) from the date on which the report was submitted to the Financial Intelligence Centre.

5.2.2.2 we reasonably require the record for lawful purposes related to our functions or activities;

These may include, but are not limited to, instances where –

(i) member banks need to retain images from a CCTV system installed to prevent fraud at an ATM for an extended period of time, since a suspicious transaction will only be identified once a victim gets their bank statement;

(ii) member banks retain the personal information of its customers for at least as long as a data subject remains its customer;

(iii) member banks need to retain personal information of former customers so that they can deal with any complaints the customer might lodge after the account has been closed; and

(iv) member banks need to retain personal information of former customers so that they can respond to any legal proceedings and regulatory investigations, compliance reviews or enquiries that may commence after the data subject is no longer a customer of the member bank;

(v) an account is dormant (i.e., the accountholder has not made any transactions against that account for a certain period of time); and

(vi) member banks retain the information about the accountholder in order to comply with its obligation to repay all unclaimed balances. The obligation or liability to repay unclaimed balances expire at 60 (sixty) years from the date the funds became classified as dormant, and records of accountholders or owners of transaction funds classified as unclaimed may be destroyed from that date.

5.2.2.3 retention of the record is required by a contract between the parties thereto; or

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

5.3 Where we have established appropriate safeguards against the records being used for any other purposes, we may retain records of personal information for periods in excess of the periods contemplated in clause 5.2.1 for –

5.3.1 historical purposes, the retention of which may include archiving and system backups;

5.3.2 statistical or research purposes, the processing and retention of which may include data analytics conducted by member banks as responsible parties, operators, or as joint responsible parties when acting together with other entities within a group of companies, provided that the personal information is de-identified when the results of the analysis or research are published;

5.4 If we have used a record of your personal information to make a decision about you, we will:

5.4.1 retain the record for such period as may be required or prescribed by law;

5.4.2 if there is no law prescribing a retention period, retain the record for a period which will afford you a reasonable opportunity, taking all considerations relating to the use of the personal information into account, to request access to the record.

5.5 We will destroy or delete a record of personal information or de-identify it as soon as reasonably practicable after we are no longer authorised to retain the record.

> If we are required to destroy or delete personal information, we will as a general rule do this in a manner that prevents its reconstruction in an intelligible form. However, absolute destruction or deletion may be impossible or impracticable as a result of limitations of technology and/or the intricate nature of information and other systems. The complex environment of interdependent and interoperable systems in the financial services and banking industry may be destabilised if records are totally deleted and this may cause systemic risk. We will therefore in such circumstances ensure that the personal information is used for historical, statistical and/or research purposes only, the use limited and that appropriate safeguards are put in place.
>
> We will ensure that –
>
> (i) we will not be able, or will not attempt, to use the personal information to inform any decision in respect of any person in a manner that affects that person in any way;
>
> (ii) no other organisation gains access to the personal information;
>
> (iii) the personal information is secured with appropriate technical and organisational security measures; and
>
> (iv) that the personal information is permanently deleted if, or when, this becomes possible.

5.6 We will restrict processing of personal information if-

5.6.1 you contest its accuracy, for a period enabling us to verify the accuracy of the information;

5.6.2 we no longer need 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;

5.6.3 the processing is unlawful, and you oppose its destruction or deletion and request the restriction of its use instead; or

5.6.4 you request to transmit the personal information into another automated processing system.

5.7 If processing of personal information is restricted as contemplated in clause 5.6 above, we will-

5.7.1 process such personal information, with the exception of storage, only for purposes of proof, or with your consent, or with the consent of a competent person in respect of a child, or for the protection of the rights of another person or if such processing is in the public interest; and

5.7.2 inform you before lifting the restriction on processing.

If we restrict personal information we will withhold from circulation, use or publication any personal information that forms part of a filing system, but not delete or destroy such personal information. This may for example be done by-

(i) temporarily moving the personal information to another processing system;
(ii) making the personal information unavailable to users; or
(iii) temporarily removing published personal information from a website.

6 FURTHER PROCESSING LIMITATION

6.1 We will further process personal information in accordance or compatible with the purpose for which it was collected.

6.2 The member banks will perform the necessary assessment to assess compatibility. This assessment will ensure that:

6.2.1 adequate safeguards are implemented to prevent unlawful further processing from taking place; and

6.2.2 the risks to the data subjects are reasonably mitigated.

6.3 In order to assess whether further processing is compatible with the purpose of collection, we will take account of-

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

6.3.2 the nature of the information concerned;

6.3.3 the consequences of the intended further processing for you;

6.3.4 the manner in which the information has been collected;

6.3.5 and any contractual rights and obligations between the parties.

6.4 The further processing of personal information is <u>not incompatible</u> with the purpose of collection if-

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

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

6.4.3 further processing is necessary-

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

6.4.3.2 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 34 of 1997;

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

6.4.3.4 in the interests of national security;

6.4.4. the further processing of the information is necessary to prevent or mitigate a serious and imminent threat to-

6.4.4.1 public health or public safety;

6.4.4.2 the life or health of the data subject or another individual;

6.4.5 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

6.4.6 the further processing of the information is in accordance with an exemption granted by the Regulator under section 37 of POPIA.

If we have obtained your personal information for a particular purpose and you have provided your consent for such personal information to be processed (or we have relied on any other lawful basis for processing your personal information), then we will not be required to obtain your consent again (or rely

on the same or another lawful basis for processing) to further process the personal information (i.e., for another purpose) provided that the further processing is in accordance or compatible with the (original) purpose for which it was originally collected. In order to determine whether such further processing is compatible with the original purpose, we will consider that set out in clause 6.2 above. The assessment for compatibility as set out in clause 6.2 above will not be required if further processing is conducted and any of the requirements set out in 6.3 above are met.

Instances of when further processing may occur include (but are not limited to):

(i) If you are a customer with a bank, and you have opened a savings account with us, we may process your personal information for purposes of opening any other account with us.

(ii) If you have an existing credit facility with a bank, we may use your personal information to assess whether you are eligible for a higher credit limit than the original credit limit agreed to and inform you. We can process your personal information again because the new purpose is compatible with the original purpose.

7 INFORMATION QUALITY

7.1 We will take reasonably practicable steps to ensure that your personal information is complete, accurate, not misleading and updated where necessary, having regard to the purpose for which personal information is collected or further processed.

7.2 We will also make available various self-service and assisted channels for you to update your personal information which we may verify against certain third-party data sources to ensure that identity theft and other fraud risk is mitigated.

7.3 Each member bank will ensure, as far as reasonably and practically possible, that the quality requirements of personal information are identified, measured, internally reported upon and that issues are resolved and mitigated (where possible).

Member banks have various requirements regarding information quality. These requirements may include the following international standards or best industry practices:

(i) King IV Code of Governance Principles

(ii) King IV Report on Governance

(iii) BASEL Principles for effective risk data aggregation and risk reporting ("**BCBS 239**")

(iv) Select International Organization for Standardization ("**ISO**") standards

8 OPENNESS

8.1 We will maintain the documentation of all processing operations under our responsibility as referred to in section 51 of PAIA.

PAIA regulates access to records held by the member banks. All member banks will provide a link to the manual required by PAIA on their websites. Insofar as POPIA is concerned, the manual will contain -

(i) the purpose of the processing (of records);

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

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

(iv) planned transborder flows of personal information; and

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

8.2 If we collect personal information, we will take reasonably practicable steps (such as enabling our employees to provide a physical copy of the notice to you at your request, or displaying a privacy notice /

statement on our website, or in our banking applications which is concise, transparent, intelligible, easily accessible and in clear and plain language) to ensure that you are aware of -

8.2.1 the information being collected and where the information is not collected from you, the source from which it is collected;

8.2.2 the name and address of the responsible party;

8.2.3 the purpose for which the information is being collected;

8.2.4 whether or not the supply of the information by you is voluntary or mandatory;

8.2.5 the consequences of failure to provide the information;

8.2.6 any particular law authorising or requiring the collection of the information;

8.2.7 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;

8.2.8 any further information such as the-

8.2.8.1 recipient or category of recipients of the information;

8.2.8.2 nature or category of the information;

8.2.8.3 existence of the right of access to and the right to rectify the information collected;

8.2.8.4 existence of the right to object to the processing of personal information. If you object to the processing of personal information, you must complete the prescribed form which can be obtained at https://inforegulator.org.za; and

8.2.8.5 your right to lodge a complaint to the Regulator and the contact details of the 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 you to be reasonable.

8.2.9 The steps referred to above will be taken-

8.2.9.1 if the personal information is collected directly from you, before the information is collected, unless you are already aware of such information;

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

8.2.10 If we have previously taken the steps referred to in clause 8.2, we will be regarded as complying with these obligations in relation to the subsequent collection from you of the same personal information or personal information of the same kind if the purpose of collection of the information remains the same.

8.2.11 We will not be required to comply with the obligations set out in clause 8.2 if –

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

8.2.11.2 non-compliance would not prejudice your legitimate interests;

8.2.11.3 non-compliance is necessary-

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

8.2.11.3.2 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 34 of 1997;

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

8.2.11.3.4 in the interests of national security;

8.2.11.3.5 compliance would prejudice a lawful purpose of the collection;

8.2.11.3.6 compliance is not reasonably practicable in the circumstances of the particular case; or

8.2.11.3.7 the information will not be used in a form in which you may be identified; or be used for historical, statistical or research purposes.

We may retain and evaluate information on your recent visits to our websites and how you move around different sections of our website for analytics purposes. Such analytics will allow us to extract

a systematic computational analysis of the data (without identifying you), so that we may understand how other data subjects will use our website and make that website more intuitive, i.e., easier to use.

We may also process your personal information for purposes of mitigating fraud by monitoring your shopping and use of ATMs in order to be able to detect an inconsistency in conduct and warn you of such conduct.

We use personal information to detect, prevent and report fraud and other financial crime. Personal information is analysed to understand trends in, types of and impacts of fraud and other financial crime. The member banks are required to perform these analytics to mitigate financial crime risks and thereby comply with the following pieces of legislation, among others:

(i) Financial Intelligence Centre Act 38 of 2001 ("**FICA**")
(ii) Prevention and Combating of Corrupt Activities Act 12 of 2004 ("**PRECCA**")
(iii) Prevention of Organised Crimes Act 121 of 1998 ("**POCA**")
(iv) Protection of Constitutional Democracy Against Terrorist and Related Activities Act 33 of 2004 ("**POCDATARA**")
(v) Financial Action Task Force Recommendations
(vi) Cybercrimes Act 19 of 2020

8.3 Security safeguards

8.3.1 We will secure the integrity and confidentiality of personal information in our possession or under our control by taking appropriate, reasonable technical and organisational measures to prevent-

8.3.1.1 loss of, damage to or unauthorised destruction of personal information; and

8.3.1.2 unlawful access to or processing of personal information.

8.3.2 We will take reasonable measures to-

8.3.2.1 identify all reasonably foreseeable internal and external risks to personal information in our possession or under our control;

8.3.2.2 establish and maintain appropriate safeguards against the risks identified;

8.3.2.3 regularly verify that the safeguards are effectively implemented; and

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

8.3.3 We will have due regard to generally accepted information security practices and procedures which may apply to us generally or be required in terms of specific industry or professional rules and regulations.

8.3.4 We will from time-to-time share information with data subjects regarding practical measures to protect their personal information. Data subjects must ensure that their personal information is protected as this is essential to prevent fraud and theft.

The member banks will ensure that people, processes, technology, and organizational controls are implemented to protect the confidentiality, integrity, and availability of personal information throughout its lifecycle as part of its ongoing risk management.

Industry standards may include, but is not limited to, the Payment Card Industry Data Security Standard ("**PCI DSS**"), which has been adopted by the banks. The PCI DSS is a set of requirements intended to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.

Member banks may also follow industry standards like the International Organization for Standardization to guide the type of controls to be considered, but specific controls are based on the risk management practices specific to each of the member banks.

People controls include ongoing training and awareness on privacy and information security matters.

8.4 ***Operator***

8.4.1 If we appoint an operator (i.e., a person who processes personal information for us in terms of a contract or mandate, without coming under our direct authority), such an operator will be obliged to-

8.4.1.1 process such information only with our knowledge or authorisation; and

8.4.1.2 treat personal information which comes to the operator's knowledge as confidential and must not disclose it, unless required by law or in the course of the proper performance of their duties.

8.4.2 In addition, we will, in terms of a written contract between us and the operator –

8.4.2.1 ensure that such an operator establishes and maintains the security measures referred to in clause 8.3 above. Such an operator will therefore be required to meet or exceed the bank's minimum requirements for data security;

8.4.2.2 oblige the operator to notify us 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.

8.5 ***Notification of security compromise***

8.5.1 We have risk management processes in place to identify any potential security compromises.

8.5.2 Any potential security compromises will be investigated to establish whether your personal information was unlawfully accessed or acquired.

8.5.3 When we have reasonable grounds to believe that your personal information has been accessed or acquired by an unauthorised person ("**security compromise**") we will notify you, as well as the Regulator, within a reasonable and appropriate time after becoming aware of the security compromise, taking into account the nature of the personal information compromised and the potential risk of harm to you.

EXAMPLE – POTENTIAL RISK OF HARM:

A potential risk of harm will be apparent where the risk may result from personal information exposed by the security compromise which could lead to physical, material, or non-material damages to the affected data subject, such as –

(i) where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal information protected by professional secrecy, unauthorised reversal of de-identified personal information, or any other significant economic or social disadvantage;

(ii) where data subjects might be deprived of their right to privacy or prevented from exercising control over their personal information;

(iii) where personal information reveals racial or ethnic origin, political persuasion, religion or philosophical beliefs, trade union membership, and the processing of biometric information, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;

(iv) where personal characteristics are disclosed, such as where we analyse or predict aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location, or movements, in order to create or use personal profiles; or

(v) where personal information of vulnerable natural persons, particularly of children, is processed.

8.5.4 Notification to you will be in writing and communicated to you in at least one of the following ways:

8.5.4.1 mailed to your last known physical or postal address;

8.5.4.2 sent by e-mail to your last known e-mail address;

8.5.4.3 placed in a prominent position on our website;

8.5.4.4 published in the news media;

8.5.4.5 published via various other online and electronic communication channels, including but not limited to an SMS to your mobile phone.

8.5.5 The notification will provide sufficient information to allow you to take protective measures against the potential consequences of the security compromise, including-

8.5.5.1 a description of the possible consequences of the security compromise;

8.5.5.2 a description of the measures that we intend to take or have taken to address the security compromise;

8.5.5.3 a recommendation with regard to the measures to be taken by you to mitigate the possible adverse effects of the security compromise; and

8.5.5.4 if known to us, the identity of the unauthorised person who may have accessed or acquired the personal information.

You can also take the following steps to protect yourself against harm should your personal information form part of a security compromise:

(i) You may register a protective registration with the South African Fraud Prevention Services ("**SAFPS**").

(ii) You could obtain your free credit bureau report from a registered credit bureau to ensure that there are no unauthorised entries on your credit bureau report.

(iii) You could obtain a report from the Registrar of Deeds to establish if there are any titles or caveats registered against your name. Please refer to https://www.mydeedsearch.co.za/deeds-office/.

(iv) You could conduct a search with the Companies and Intellectual Property Commission ("**CIPC**") to establish whether you have any exposure to a registered entity. The CIPC website address is http://www.cipc.co.za/za/.

9 **DATA SUBJECT PARTICIPATION**

9.1 You, having provided adequate proof of identity, have the right to-

9.1.2 request us to confirm, free of charge, whether or not we hold personal information about you; and

9.1.3 request from us the record or a description of the personal information about you held by us, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information –

9.1.3.1 within a reasonable time;

9.1.3.2 at a prescribed fee, if any. If we require you to pay a fee, we will give you a written estimate of the fee before providing the services, and may require you to pay a deposit for all or part of the fee;

9.1.3.3 in a reasonable manner and format; and

9.1.3.4 in a form that is generally understandable.

9.2 In response to such a request, we will advise you of your right to request the correction of information as set out in clause 9.4 below.

9.3 We may or must refuse, as the case may be, to disclose any such information requested 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 PAIA apply. We also advise that the provisions of section 61 of PAIA are applicable in respect of access to health or other records. If access to any part of the information may or must be refused, every other part must be disclosed.

9.4 You may, in the prescribed manner (the prescribed form can be obtained at https://www.justice.gov.za/inforeg/), request us to-

9.4.1 correct or delete personal information about you in our possession or under our control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully; or

9.4.2 destroy, delete, or de-identify a record of personal information about you that we are no longer authorised to retain.

9.5 On receipt of your request, we will, as soon as reasonably practicable-

9.5.1 correct the information;

9.5.2 destroy, delete or de-identify the information;

9.5.3 provide you with credible evidence in support of the information; or

9.5.4 where agreement cannot be reached, and if you so request, 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.

9.6 If we have taken the steps under clause 9.5 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 you, we will, if reasonably practicable, inform each person or body or responsible party to whom the personal information has been disclosed of those steps.

9.7 We will notify you of any action taken as a result of your request.

9.8 Your rights under this clause may not be absolute and may be limited where the law requires or permits such limitation.

You understand that if your request us to delete personal information and we rely on that personal information to provide you with services or products, then we will not be able to provide you with such products and services. "Free of charge" means that we will not charge you. The communication channel that you use may however charge you a fee for use of airtime or charge for data costs.

B PROCESSING OF SPECIAL PERSONAL INFORMATION

10. PROHIBITION ON THE PROCESSING OF SPECIAL PERSONAL INFORMATION

10.1 Special personal information is personal information concerning-

10.1.1 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

10.1.2 the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

10.2 We may process your special personal information, provided that -

10.2.1 you consented to the processing; or

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

The Employment Equity Act 55 of 1998 and the Broad-Based Black Economic Empowerment Act 53 of 2003 contains provisions regarding the employment of people who have disabilities and sets targets for businesses for the employment of black people with disabilities. For purposes of complying with this legislation, banks will process the health information of its employees. The Southern African Fraud Prevention Service ("**SAFPS**") is a non-profit company committed to combating fraud across the financial services industry by providing a shared database to member organisations as well as offering the South African public a means of protecting themselves against impersonation and identity theft. Banks report and file cases of confirmed or suspected fraud onto the database held by SAFPS. For more information on SAFPS their website can be visited at: https://www.safps.org.za/.

10.2.3 processing is necessary to comply with an obligation of international public law; or

10.2.4 processing is for historical, statistical or research purposes to the extent that-

10.2.4.1 the purpose serves a public interest, and the processing is necessary for the purpose concerned; or

10.2.4.2 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 data subject to a disproportionate extent; or

10.2.5 you have deliberately made the information public.

10.3 ***A data subject's race or ethnic origin***

10.3.1 The processing of the personal information concerning a data subject's race or ethnic origin, may occur if the processing is carried out to-

10.3.1.1 identify data subjects and only when this is essential for that purpose; and

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

We may process your personal information concerning race or ethnic origin in accordance with the applicable laws, including but not limited to -

(i) The Home Loans and Mortgage Disclosure Act of 63 of 2002 established an Office of Disclosure. Financial institutions are obliged to make certain reports to this Office, including the race of an applicant. Such records must be kept for a period of at least 3 (three) years from the time the report if first furnished to the Office.

(ii) The Broad-Based Black Economic Empowerment Act 53 of 2003 required that all public companies listed on the Johannesburg Stock Exchange must provide to the Broad-Based Black Economic Empowerment Commission established by section 13B, in such manner as may be prescribed, a report on their compliance with broad-based black economic empowerment.

(iii) Labour legislation which contains provisions regarding the employment of people who have disabilities and sets targets for businesses for the employment of black people with disabilities. For purposes of complying with this legislation, member banks will process the health information of its employees or prospective employees.

10.4 ***A data subject's criminal behaviour or biometric information***

10.4.1 The processing of personal information concerning a data subject's criminal behaviour or biometric information, may occur if the processing is carried out by bodies charged by law with applying criminal law or by member banks who have obtained that information in accordance with the law.

10.4.2 The processing of information concerning personnel in the service of the responsible party will take place in accordance with the rules established in compliance with labour legislation.

10.4.3 The processing of any of the categories of personal information referred to clause 10.1. may occur if such processing is necessary to supplement the permitted processing of information on criminal behaviour or biometric information.

We may process your personal information concerning your criminal behaviour or biometric for the following reasons (which are not intended to be exhaustive)-

(i) The Department of Home Affairs is the custodian of the Home Affairs National Identity System ("**HANIS"**). HANIS may be used by member banks to verify your identity online by placing your finger on a biometric reader which will read your finger against the Department of Home Affairs' data base.

(ii) The usage of the fingerprint of the data subject to identify the data subject for the purposes of establishing a relationship or processing a financial transaction/payment transaction. This processing is conducted in compliance with legislation – like the Financial Intelligence Centre Act 38 of 2001 ("**FICA**").

(iii) Engagements with data subjects over the telephone is recorded. These recordings take place in compliance with the Financial Advisory and Intermediaries Services Act 37 of 2002 ("**FAIS Act**") among others.

(iv) Facial recognition is also used to prevent fraud and other crimes. It identifies the data subject and verifies the identity of the data subject. This processing takes place in compliance with legislation.

(v) The Southern African Fraud Prevention Service ("**SAFPS**") is a non-profit company committed to combating fraud across the financial services industry by providing a shared database to

member organisations as well as offering the South African public a means of protecting themselves against impersonation and identity theft. Banks report and file cases of confirmed or suspected fraud onto the database held by SAFPS. For more information on SAFPS their website can be visited at: https://www.safps.org.za/.

10.5 Each member bank will internally monitor compliance with this clause of the Code, including the relevant provisions of POPIA. The accountability section of this Code would apply here.

C PROCESSING OF PERSONAL INFORMATION OF CHILDREN

11 PROHIBITION ON PROCESSING PERSONAL INFORMATION OF CHILDREN

11.1 A bank as a responsible party may, except as set out in clause 11.2 and clause 11.3 below, not process personal information concerning a child.

11.2 The prohibition on processing personal information of children, does not apply if the processing is-

11.2.1 carried out with the prior consent of a competent person;

11.2.2 necessary for the establishment, exercise, or defence of a right or obligation in law;

11.2.3 necessary to comply with an obligation of international public law;

11.2.4 for historical, statistical or research purposes to the extent that-

11.2.4.1 the purpose serves a public interest, and the processing is necessary for the purpose concerned; or

11.2.4.2 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

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

11.3 ***Opening and managing the accounts of minors.***

11.3.1 Despite the provisions of sections 34 and 35 of POPIA and in terms of section 87 of Banks Act 94 of 1990 we will allow a minor over the age of 16 years and under the age of 18 who is not emancipated or married, to make a deposit at a bank (i.e., be a depositor) without requiring the consent or assistance of a competent person, i.e., any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning the minor.

11.3.2 Such minors may therefore without the consent or assistance of a competent person, execute all necessary documents, give all necessary acquittances and cede, pledge, borrow against, and generally deal with, that minor's deposit as the minor thinks fit; and will enjoy all the privileges and be liable to all the obligations and conditions applicable to depositors.

11.3.3 We will process the personal information of such minors for the specific purpose of opening and managing the accounts and in accordance with all of the conditions for lawful processing of personal information as contemplated in Chapter 3 of POPIA.

11.4 Each member bank will internally monitor compliance with this clause of the Code, including the relevant provisions of POPIA. The accountability section of this Code would apply here.

D DIRECT MARKETING

12 DIRECT MARKETING

12.1 We may process your personal information for the purpose of direct marketing by means of -

12.1.1 any form of electronic communication, including automatic calling machines (i.e., a machine that is able to do automated calls without human intervention), SMSs or e-mail; and

12.1.2 other methods such as voice (telephone or video call), in person or by post, provided that we comply with applicable laws;

12.2 We will not directly market to you using electronic communications (as referred to in clause 12.1.1) unless you-

12.2.1 have given us your consent to the processing; or

12.2.2 are, subject to clause 12.4, our customer.

12.3 We may approach you if your consent is required in terms of clause 12.1.1 and you have not previously withheld such consent, only once in order to request your consent.

12.4 A member bank may only process your personal information if you are a customer of that bank, -

12.4.1 if your contact details were obtained-

12.4.1.1 in the context of the sale of a product or service, including –

12.4.1.1.1 where you agree to a product or service being provided to you and we do not charge you for that product or service;

12.4.1.1.2 if you or we declined the offer of a product or service made to or by you; and

12.4.1.1.3 where you concluded an agreement with us regarding the product or service offered to you.

12.4.2 for the purpose of direct marketing of the member bank's products and services or the products and services offered together with other entities in the group of companies to which the member bank belongs (i.e., as joint responsible parties); and

12.4.3 if you have been given a reasonable opportunity to object, free of charge, and in a manner free of unnecessary formality (which will be as simple as reasonably possible), to such use of your electronic details at the time when the information was collected; and on the occasion of each communication with you for the purpose of marketing if you have not initially refused such use.

12.5 Any communication for the purpose of direct marketing must contain-

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

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

The member banks may obtain consent for unsolicited electronic direct marketing via any form of electronic communication or non-electronic communication.

Member banks will request your consent by -

(i) addressing you, and this may be in a formal or informal mode;
(ii) including our contact details (such as an address, contact number or email address);
(iii) referring to the products, goods, or services the consent relates to;
(iv) giving examples of the forms of the electronic communication to which the consent relates;
(v) including the date; and
(vi) include a requirement for you to sign or accept.

If you engage with us on our channels, then you will be informed of who the responsible party is, and the details and signature of the designated person will not be required.

E AUTOMATED DECISION-MAKING

13 AUTOMATED DECISION-MAKING BY MEMBER BANKS

13.1 We may make use of automated decision-making to provide a profile of a data subject, including his or her performance at work, or his or her credit worthiness, location, health, reliability, personal preferences, or conduct.

13.2 We will identify all of our processes that use automated decision making as defined in this Code.

13.3 We will assess whether the identified processing is lawful in terms of POPIA and this Code.

13.4 We will implement safeguards appropriate for the identified processes.

13.5 We will ensure that data subjects are informed of their rights in respect of automated decision making. This will be achieved by the privacy notices/statements on our websites.

13.6 We will embed processes, that will be reviewed and amended where needed, to give effect to the data subject rights to make representation about an automated decision.

13.7 We will monitor automated decision making as part of our ongoing risk management frameworks.

13.8 Where automated decision-making is employed in the processing of personal information, we will, in protecting the legitimate interests of a data subject –

13.8.1 notify the data subject that the processing of personal information may be subject to automatic decision-making;

13.8.2 provide to the data subject sufficient information about the personal information which was used as well as how and why we arrived at the decision; and

13.8.3 inform the data subject of processes available to enable the data subject to make representations relating to the automated decision-making and provide the data subject a reasonable opportunity to make representations to us. This will be achieved via each member bank's privacy notice / statement available on its website.

13.9 If you are dissatisfied with the result of an automated decision, you are also entitled to make use of the complaints procedures set out in Section I below.

13.10 You understand that you may be refused access to information in terms of PAIA as set out in our PAIA Manuals which are available on our websites.

F INFORMATION MATCHING PROGRAMMES

14 INFORMATION MATCHING

14.1 If we make use of an information matching programme, we will –

14.1.1 ensure that we do so in a manner that complies with POPIA;

14.1.2 ensure that the algorithms used to match the information has been externally validated and reviewed to ensure that they are valid, useful, fair, and appropriate;

14.1.3 put measures in place to regularly assess the quality of the personal information used in the information matching programme;

14.1.4 provide all data subjects whose personal information is used in the matching programme meaningful access to the personal information used and create the opportunity for data subjects to make representations about the accuracy of the information, unless access is prohibited by applicable laws or good industry practices; and

14.1.5 ensure that if a negative result is generated (e.g., the information matching programme reveals that a person provided us with incorrect personal information) the information is not used in making a significant decision about the data subject before the data subject is informed of the negative result and given an opportunity to make representations unless the bank is prohibited by applicable laws from informing the data subject.

We make use of information matching programmes to comply with the Financial Intelligence Centre Act 38 of 2001 ("**FICA**"). Member banks are required to conduct customer due diligence ("**CDD**"), on their customers and screen customers against watch lists, in accordance with their risk management and compliance programme, which governs the manner in which the member banks will comply with their obligations as set out in FICA. A bank may request the assistance of another bank to provide it with CDD information and/or documentation in relation to shared customers for the purposes of establishing and verifying the identity of the customers.

G AUTHORITY

15 AUTHORISATIONS

15.1 The Regulator has issued this Code in terms of chapter 7 of POPIA after application was made by BASA, representing the member banks. Member banks are therefore exempt from requesting prior authorisation as contemplated in section 57 of POPIA and we are not required to notify the Regulator of such processing.

15.2 In particular, we may process- -

15.2.1 any unique identifiers of data subjects-

15.2.1.1 for a purpose other than the one for which the identifier was specifically intended at collection; and

15.2.1.2 with the aim of linking the information together with information processed by other responsible parties.

> A '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, such as your account number.

15.2.2 information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;

> If a bank is part of a group of companies and some of those companies are also accountable institutions as contemplated under the Financial Intelligence Centre Act 38 of 2000 ("**FICA**"), then such a bank may process personal information on criminal behaviour or unlawful or objectionable conduct on behalf of those other accountable institutions, so that all such accountable institutions may comply with customer due diligence and reporting obligations under FICA.

15.2.3 information for the purposes of credit reporting;

> Member banks are also members of the South African Credit and Risk Reporting Agency which facilitates the sharing of credit and risk data with its associate member credit bureaux enabling banks to comply with credit information sharing provisions of the National Credit Act 34 of 2005, as well as the provisions for performing credit and risk assessments and affordability calculations.

15.2.4 the transfer of special personal information, as referred to in section B of this Code, or the personal information of children as referred to in section C of this Code, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information as referred to in section H of this Code.

15.3 Each member bank will monitor compliance with this clause of the Code, including the relevant provisions of POPIA. The accountability section of this Code would apply here.

H TRANSBORDER FLOW OF INFORMATION

16. TRANSFER OF INFORMATION

16.1 A responsible party in South Africa may not transfer personal information about a data subject to a third party who is in a foreign country unless-

16.1.1 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-

16.1.1.1 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

16.1.1.2 includes provisions, that are substantially similar to this clause, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;

16.1.1.3 the data subject consents to the transfer;

16.1.1.4 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;

> In the following instances (which is not intended to be an exhaustive list) we may transfer your personal information because it is necessary for the performance of an agreement between us –
>
> (i) you use your credit card in a foreign country to make purchases;
>
> (ii) you have a foreign currency account and instruct us to transfer money to that account; and
>
> (iii) you are party to an agreement with a lender/s and/or counterparty/ies that is/are domiciled in a foreign country.

16.1.1.5 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

16.1.1.6 the transfer is for the benefit of the data subject, and-

16.1.1.7 it is not reasonably practicable to obtain the consent of the data subject to that transfer; and

16.1.1.8 if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

Many banks are part of a group of companies and the holding company of that group of companies may prescribe binding corporate rules for all the subsidiaries in that group of companies. If those binding corporate rules provide an adequate level of protection as set out in clause 16.1.1 above, then the personal information of a data subject may be transferred to a subsidiary in a foreign country.

I COMPLAINTS

17 INTERNAL DISPUTE RESOLUTION

17.1 If you have a complaint because you are dissatisfied with the result of an automated decision, about compromised personal information, or about our compliance with this Code, you must **first** raise this with the responsible party in accordance with the complaints management framework of the member banks as set out below.

17.2 All member banks are obliged to establish, maintain, and operate an adequate and effective complaints management framework to ensure the fair treatment of complainants and that complies with the Conduct Standards for Banks, 2020, as published by the Financial Sector Conduct Authority under the Financial Sector Regulation Act 9 of 2017.

17.3 In accordance with this Conduct Standard the member banks are obliged to establish and maintain an appropriate internal complaints escalation and review process. We (the banks) will ensure that our complaint processes and procedures are transparent, visible, and accessible through all appropriate channels.

17.4 ***Complaints management framework of the member banks.***

17.4.1 Where a complaint is upheld, any commitment by us to make a compensation payment, goodwill payment or to take any other action will be carried out without undue delay and within any agreed timeframes.

17.4.2 Where a complaint is rejected, you (as the complainant) will be provided with clear and adequate reasons for the decision and must be informed of any applicable escalation or review processes, including how to use them and any relevant time limits.

17.4.3 We are obliged to ensure accurate, efficient, and secure recording of complaints-related information.

17.4.4 We will not impose any charge for you to make use of our complaint processes and procedures.

17.4.5 We will, within a reasonable time after receipt of a complaint, acknowledge receipt thereof and promptly inform you of the process to be followed in handling the complaint, including-

17.4.5.1 the contact details of the person or department that will be handling the complaint;

17.4.5.2 indicative timelines for addressing the complaint;

17.4.5.3 details of the internal complaint's escalation and review process if you are not satisfied with the outcome of a complaint; and

17.4.5.4 details of escalation of complaints to the office of the Ombudsman for Banking Services or independent adjudicator as contemplated below.

17.4.6 You will be kept adequately informed of -

17.4.6.1 the progress of the complaint;

17.4.6.2 causes of any delay in the finalisation of the complaint and revised timelines; and

17.4.6.3 our decision in response to the complaint.

18 OMBUDSMAN FOR BANKING SERVICES

18.1 If we do not resolve your dispute, or you are not satisfied with the outcome of our complaints handling process, you are welcome to make use of the services of the Ombudsman for Banking Services. We will

also, where relevant, give you information on other Ombudsman offices or independent adjudicators, which might have jurisdiction over your complaint.

18.2 An independent Ombudsman for Banking Services Office has been established. The Ombudsman for Banking Services is available at no cost to you to consider any complaint that we have not been able to resolve with you.

18.3 The Ombudsman for Banking Services is entitled to mediate, make a determination based on this Code or on the law where the law is reasonably certain or make a recommendation in other circumstances including those based on equity. If we decline to accept any recommendation made by the Ombudsman for Banking Services, then the Ombudsman may, at her discretion, publish the fact that a recommendation was made, and we have refused to accept it. A determination made by the Ombudsman for Banking Services may be made an order of the court.

18.4 All banks that are members of BASA are automatically subject to the jurisdiction of the Ombudsman for Banking Services. We will supply you with the Ombudsman for Banking Service's brochure, address and telephone numbers on request and we will ensure that the Ombudsman for Banking Service's contact details are prominently displayed in our branches (if applicable). If we fail to resolve your dispute with us, or at your request, we will provide you with the documentation required to lodge a complaint with the Ombudsman for Banking Service's Office.

18.5 If the Ombudsman for Banking Services is unable for whatever reason to hear your complaint, we will through BASA appoint an independent adjudicator as set out below.

18.6 The Ombudsman for Banking Services will follow its Terms of Reference when adjudicating upon a complaint. The Terms of Reference is available at www.obssa.co.za.

19 INDEPENDENT ADJUDICATORS

19.1 BASA may appoint one, or if it deems necessary, more than one independent adjudicator to hear the complaint and adjudicate thereon.

19.2 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.

19.3 The adjudication of the complaint will take place in Johannesburg and in accordance with the rules of the Arbitration Foundation of Southern Africa's domestic arbitration rules. These rules can be found at https://arbitration.co.za/.

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

19.5 Any adjudication of a complaint in terms of this clause will be conducted in camera and the parties involved will treat it as confidential and not disclose to any third-party details of the complaint submitted for adjudication, the conduct of the adjudication proceedings or the outcome of the adjudication, without the written consent of all the parties.

19.6 On completion of his or her investigation the independent adjudicator must send a report containing its determination, together with reasons therefor, to BASA and the relevant bank.

19.7 If the bank is determined to be in breach of this Code the adjudicator may make or give any order, declaration or direction requiring that the bank takes any specific actions within a reasonably stipulated period of time.

19.8 The independent adjudicator will submit a report to the Regulator annually.

19.9 The report must contain at a minimum the following information:

19.9.1 The functions the independent adjudicator has performed under this Code for that past year; and

19.9.2 The number and nature of the complaints made to the independent adjudicator under the Code for that past year.

20 THE REGULATOR

20.1 A responsible party or data subject who is aggrieved by a determination, including any declaration, order or direction that is included in the determination, made by either the Ombudsman for Banking Services or an independent adjudicator appointed by BASA as set out above, after having investigated a complaint relating to the protection of personal information under this Code, may submit a complaint in terms of section 74(2) of POPIA with the Regulator, against the determination upon payment of a prescribed fee.

20.2 The complaint can be escalated directly to the Regulator in instances where the complaint warrants the attention of the Regulator, including and not limited to the following circumstances:

20.2.1 The complainant will be disadvantaged if the complaint is directed to the responsible party directly;

20.2.2 a systemic violation of the protection of personal information has occurred;

20.2.3 the responsible party has a history of habitual violation of the protection of personal information;

20.2.4 complainants represent a class of individuals against the same responsible party; or

20.2.5 the complaints arise out of similar circumstances and there is a common issue of law or fact.

J GENERAL

21 REVIEW AND EXPIRY OF THE CODE.

21.1 We may review this Code annually and apply for approval by the Regulator for any variations that may result from such a review.

21.2 If the Regulator has provided its approval, we will publish the varied Code on our website within 14 (fourteen) days from the date of publication of the varied Code in a Government Gazette.

21.3 The Regulator may on its own initiative review the operation of an approved code within a 5 (five) year period or as and when deemed necessary. We will consult with the Regulator during such a review process and inform you of the outcome.

21.4 This Code shall in any event expire within a minimum period of 5 (five) years. We shall take such steps as may be necessary to apply for the approval of a new Code before the expiry of the current Code.

K ANNEXURE

For ease of reference, the important websites of relevance to this Code have been listed below:

www.banking.org.za
www.obssa.co.za
https://arbitration.co.za/
https://www.safps.org.za/
http://www.cipc.co.za/za/
https://www.mydeedsearch.co.za/deeds-office/
https://www.justice.gov.za/inforeg/
www.fic.gov.za/