



DATA SUBJECT PARTICIPATION (“DSP”) MANUAL

Protection of Personal Information (“POPI”) Act No 4 of 2013

Table of Contents

1. Purpose, Scope and Users.....	3
2. Applicable Legislation	3
3. Data Subject Participation (“DSP”) request	4
4. The Rights of a Data Subject	4
5. Requirements for a valid DSP	5
6. DSP Process	5
6.1 Request.....	5
6.2 Identity verification.....	5
6.3 Information for Data Subject Participation request	5
6.4 Review of Information	6
6.5 Response to Access Requests	6
6.6 Archiving.....	6
6.7 Disposal.....	6
7. Exclusions	6
8. Data Subject Access Request Refusals	7
9. Responsibilities	8
10.Availability of this Manual.....	8
11.Annexure A (Form 2).....	8

1. Purpose, Scope and Users

The purpose of this document is to set out the key features for the handling or responding to requests for access or deletion of personal data made by data subjects, their representatives of any other interested party. This manual enables African Bank Limited (“the Bank”) to act in accordance with legislative obligations, enable data subjects to verify that information held about them is correct and afford data subjects the opportunity to have information about them deleted where such request qualifies for deletion within the legal framework.

This manual applies broadly across the Bank and group companies.

This manual applies to data subjects and Bank employees that handle data subject access requests such as a Regulatory Officer.

2. Applicable Legislation

Records are kept in accordance with such other legislation as is applicable to the Bank and group companies, which include but is not limited to the following:

- Protection of Personal Information Act 4 of 2013;
- Promotion of Access To Information Act 2 Of 2000;
- Banks Act 94 of 1990 as amended;
- Companies Act 71 of 2008 as amended;
- National Credit Act 34 of 2005 as amended;
- Consumer Protection Act 68 of 2008;
- Long Term Insurance Act 52 of 1998;
- Electronic Communication and Transaction Act, 25 of 2002
- Pension Funds Act 24 of 1956;
- Labour Relations Act 66 of 1995;
- Basic Conditions of Employment Act 75 of 1997;
- Employment Equity Act 55 of 1998;
- Skills Development Levies Act 9 of 1999;
- Unemployment Insurance Act 63 of 2001;
- Compensation for Occupational Injuries and Diseases Act 130 of 1993;
- Policy Holder Protection Rules;
- Magistrates Court Act 59 of 1959;
- Financial Intelligence Centre Act 38 of 2001;
- Income Tax Act 58 of 1962;
- Debt Collectors Act 114 of 1998;
- Financial Advisory and Intermediary Services Act 37 of 2002.

3. Data Subject Participation (“DSP”) request

Chapter 3, Condition 8, section 23 to 25 of POPIA deals with Data Subject Participation (“DSP”). DSP is any request made by an individual or an individual’s legal representative for information held by the Bank about that individual. DSP provides the right for data subjects to see or view their own personal data, as well as to request copies of the data, and the right for their personal data to be corrected/deleted/destroyed.

DSP requests must be made in writing. Verbal requests for correction, deletion or destruction of information held about an individual are not valid DSP request. In the event a formal DSP request is made verbally to a staff member of the Bank, further guidance should be sought from the Regulatory Officer, who will consider and approve all DSP request applications.

A DSP request can be made via any of the following methods: email to Privacy@africanbank.co.za, the branch or call centre. The Bank will not provide personal information via social media channels.

4. The Rights of a Data Subject

The rights to data subject access include the following:

- The right to be notified that personal information is being collected; and
- Personal information has been accessed or acquired by an unauthorised person.
- The right to establish whether a responsible party holds information of the data subject and request access to his/her personal information.
- The right to request corrections, deletion or destruction of personal information.
- The right to object:
on reasonable grounds relating to his/her particular situation to the processing of his/her own personal information to the processing of personal information at any time for the purposes of direct marketing
- The right to not have personal information processed for the purposes of direct marketing by means of unsolicited electronic communication.
- The right to not be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his/her personal information intended to provide a profile
- The right to submit a complaint to the regulator regarding an alleged interference with the protection of the personal information
- The right to institute civil proceedings regarding the alleged interference.

The Bank must comply with a DSP request without undue delay and within one calendar month (30 days) of receipt on any information requested.

5. Requirements for a valid DSP

In order to be able to respond to the Data Subject Participation requests in a timely manner, the data subject should:

- Submit his/her request via a branch or the Service Contact Centre, or submit same using a Data Subject Access Request Form 2 (enclosed herewith per Annexure A).
- Allow the Bank to validate his/her identity via telecommunication, or biometric verification in branch (to ensure that the person requesting the information is the data subject).
- Submit a request per the PAIA process if the DSP request is via an individual's legal representative.

6. DSP Process

6.1 Request

Upon receipt of a DSP request, the Regulatory Officer will acknowledge the request. The requestor may be asked to complete a Data Subject Access Request Form (FORM 2) should the request relate to the correction, deletion or destruction of personal information. Any request made by a data subject should be made on the basis of the personal information in question being inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.

6.2 Identity verification

The Regulatory Officer needs to verify the identity of anyone making a DSP request to ensure information is only given to the person who is entitled to it. This verification will be conducted via a telephonic interaction during which a number of security questions will be asked, or through biometric verification at an African Bank branch.

If the requestor is not the data subject, access to records held by the Bank may be accessed by requesters only once the prerequisite requirements for access have been met in terms of The Promotion of Access to Information Act, No 2 of 2000 -

https://www.africanbank.co.za/media/53483/PAIA-Manual_V1.3_July_2021.pdf.

6.3 Information for Data Subject Participation request

Upon receipt of the request and/or required documents, the Regulatory Officer will notify the requestor that his/her DSP request will be responded to within 30 calendar days. The 30 day period begins from the date that the request with satisfactory documents (if required) are received. The requestor will be informed by the Regulatory Officer in writing if there will be any deviation from the 30 day timeframe due to other intervening events.

6.4 Review of Information

The Regulatory Officer will assess the request in relation to any prevailing legislation. The Regulatory Officer will determine whether there is any information which may be subject to an exclusion and/or if consent is required to be provided from a third party.

The Regulatory Officer must ensure that the information is reviewed/received/correct/deleted or destroyed (depending on the DSP request) to ensure the 30 calendar day timeframe is not breached.

6.5 Response to Access Requests

The Regulatory Officer will provide a written response to the requestor via email. Responses will be based on the information retrieved and will further encumber if the Bank does not hold the information requested, or if an exclusion applies. The Bank will only provide information via secure channels.

6.6 Archiving

After the response has been sent to the requestor, the DSP request will be considered closed and archived by the Regulatory Officer. Archive does not mean destroy. Records can be captured, kept and maintained only which are relevant to the purpose. Security controls in place will ensure the data subject's information will not be processed or uploaded once the request has been approved.

6.7 Disposal

A key element of disposal is to ensure that duplicates are also destroyed as they are also Personal Information. Duplicates could be in paper or electronic formats.

7. Exclusions

The Act does not apply to the processing of personal information *inter alia*:

- in the course of purely a personal or household activity;
- where the information has been depersonalised and the information cannot be re-identified;
- by or on behalf of a public body which may involve *inter alia* national security, combating of money laundering activities, investigations of proof of offenders etc.
- by the Cabinet and its committees or the Executive Council of a province; or
- relating to the judicial functions of a court referred to in section 166 of the Constitution

Condition 8, Part B refers to the prohibition of processing of special personal information (including religious beliefs, health information, biometric information, etc.) or criminal behaviour. The only exceptions that apply include:

- If the data subject provided consent
- If processing is necessary for establishing a defence of a right

- If processing is required for fulfilling obligations under international public law
- If processing is in the public interest
- If the data is already public (through the data subject correctly)
- If processing involves historical research, or statistical purposes (within the public interest or if asking consent is impossible or close to impossible)

Part C deals with the **data of children**. Responsible parties may not process children's personal information unless:

- A "competent person" has consented
- It is necessary for obligations under the law
- It is required for upholding international public law
- It is necessary for research purposes

In principle, the Bank will not normally disclose the following types of information in response to a DSP request:

- Information about other people – A DSP request may cover information which relates to an individual or individuals other than the data subject. Access to such data will not be granted, unless the individuals involved consented to the disclosure of their data.

The Bank will not action a deletion/destruction request should the DSP request not comply with the various legislative retention periods.

8. Data Subject Access Request Refusals

While it's important to respond to most DSP requests, the Bank does not have to respond to everyone. The Bank can refuse to comply for two reasons:

- The request is unfounded i.e. the requester does not intend to exercise their right of access appropriately.
- The request is excessive i.e. the request overlaps with another recently submitted request.

The Bank will not create a blanket policy that sets criteria for "acceptable" DSP requests. Each request must be considered on a case-by-case basis.

If the Bank decides to refuse a DSP request, the Bank will without undue delay inform the data subject or requestor about:

- The refusal or reason for not taking action; and
- The data subject's right to lodge a complaint with the Information Regulator.

9. Responsibilities

The overall responsibility for ensuring compliance with a DSP request rests with the Regulatory Officer.

It is the responsibility of a Bank employee interacting with a data subject to inform the data subject on the process to follow to make a DSP request.

Non-compliance to POPI is an offense and can result to a fine being imposed. The Regulator may apply administrative fines not to exceed R10 million. The total fine is subject to the Regulator's discretion

10. Availability of this Manual

This manual is available for inspection by the general public upon request, during office hours and free of charge at the offices of African Bank Limited.

This manual is also published on African Bank's website.

11. Annexure A (Form 2)

FORM 2

REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR
DESTROYING OR DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS
OF SECTION 24(1) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013
(ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION,
2018

[Regulation 3]

Note:

1. Affidavits or other documentary evidence may be attached to support your request.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as applicable.

Mark the appropriate box with an "x".

Request for:

- Correction or deletion of personal information which is in possession or under the control of African Bank.
- Destroying or deletion of personal information which is in possession or under the control of African Bank, who is no longer authorised to retain the record of information.

A PERSONAL DETAILS	
Name(s) and surname/ registered name:	
Identity Number:	
Residential, postal or business address:	Code ()

Contact number(s):	
Fax number/Email address:	

B INFORMATION TO BE CORRECTED/DELETED/DESTROYED

C

REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF AFRICAN BANK; and or

REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1)(b) WHICH AFRICAN BANK IS NO LONGER AUHORISED TO RETAIN.

Signed atthis day of20.....

Signature of requestor/ designated person