

# AFROCENTRIC GROUP DATA PRIVACY POLICY

## **PART VII - INTERNAL AND CROSS BORDER DISCLOSURE OF PERSONAL AND SPECIAL PERSONAL INFORMATION BY THE GROUP ON ITS WEBSITES**

The Personal and Special Personal Information of Data Subjects that is collected by the Group on its respective websites shall not be shared with or transferred to companies and/or person affiliated, associated and in business with the Group, irrespective of their location in the world, unless such sharing or transfer is done in accordance with the provisions of the POPIA and Applicable Data Protection Legislation.

All data stored within the Group, is stored within controlled servers where access is limited.

Personal and Special Personal Information may be stored and processed in South Africa or any other country where the Group, its partners, affiliates or agents are located, provided that those other countries have legislation protecting the Personal Information at least the same level as contemplated by POPIA.

The Group may send Personal Information to external companies or people under any of the following circumstances:

- i. when consent has been obtained to share the information;
- ii. when the Group is required to provide information to the user in respect of products or service requested by the user;
- iii. when the Group is required to send the information to service providers who work on its behalf to provide a product or service to the user (we will only provide the information if the service provider needs to deliver the service and the information shall only be shared for such particular purpose and on the strict understanding that they are prohibited from using the information for any other purpose);
- iv. when the Group is requested to keep the user up to date on the latest announcements, updates, special offers or other information we think you would like to hear about either from us or our business partners (unless you have opted out of these types of communication);
- v. personal information will be disclosed if it is permitted by law to do so;
- vi. to enable us to enforce our Terms and Conditions of Use;
- vii. in urgent circumstances in order to protect personal safety, public safety or where the integrity of our website may be compromised.

## TABLE OF CONTENTS

This is the overarching Data Privacy Policy of the Group which comprises of different components and its contents are as follows:

GROUP

### GROUP DATA PRIVACY POLICY

1. Background.....	2
2. Policy Statement .....	3
3. Policy Objectives.....	4
4. Scope Of Application.....	5
5. Relevant Legislation.....	6
6. Related Policies .....	7
7. Definition Of Terms .....	7
8. Policy Provisions.....	10
8.1 Roles	12
8.2 Policy Principles	13
8.3 Prior Authorisation	35
8.4 Internal And Cross Boarder Disclosure Of Personal And Special Personal Information by The Group on Its Websites	1
8.5 Third Parties Websites	2
8.6 Agents Or Service Providers	31
8.7 Business Transfers	31
8.8 Legal Requirements	32
8.9 Security Of Personal And Special Personal Information	32
8.10 Children And Privacy	32
8.11 Breaches Notification	33
8.12 Group Information Officer	33
9. Policy Review.....	35
10. Grievance Procedure .....	36
11. Right To Lodge A Complaint To The Information Regulator .....	36
12. Monitoring And Enforcement .....	36
13. Policy Approval .....	36
Annexure A.....	37
<b>Retention Schedule .....</b>	<b>37</b>
<b>Relevant Legislation For Data Retention .....</b>	<b>46</b>

## 1. BACKGROUND

### PART VIII – MISCELLENAIOUS

#### A. Third parties' websites

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 2
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

The AfroCentric Group (or “the Group”) consists of AfroCentric Investment Corporation Limited (1988/000570/06), a Johannesburg Stock Exchange listed holding company and its subsidiaries.

AfroCentric Health (Proprietary) Limited, a subsidiary of the holding company, hosts the Group’s Corporate Head Office whose mandate is to enforce, manage and monitor, among other things, governance in alignment with the Group’s strategy and values. The AfroCentric Group’s purpose is to enhance the quality of life for our stakeholders. In order to do so, the Group is committed to ensuring that in bringing its stakeholders quality of life, it does so within the parameters of value-enhancing governance. Some of the most important pillars of governance is integrity and transparency. The Group is therefore entrusted with the responsibility of creating and enforcing an organisational wide data privacy and security compliance framework as informed by the Protection of Personal Information Act, 2013 (“POPIA”). The framework includes the implementation of this Privacy Policy.

In the course of its business activities the Group processes Personal and Special Personal Information of Data Subjects, including that of its employees, contractors, clients, medical scheme beneficiaries, service providers, business partners (“the Stakeholders”) for the purposes of meeting the Group’s business objectives and to fulfil and comply with legal and contractual obligations and enforce its legal rights.

The AfroCentric Group recognises and supports the right to privacy as a fundamental right, including the rights of Data Subjects to control the disclosure of their Personal Information. Accordingly, our stakeholders’ privacy and trust are extremely important to us. the Group is committed to ensuring that personal information (“information”) is collected and managed in a transparent and lawful manner in alignment with the POPIA

The AfroCentric Group supports local, international laws and regulations including but not limited to General Data Protection Regulation (GDPR) that seek to protect the privacy rights of all Data Subjects within and beyond the territory of the Republic of South Africa.

### **2. POLICY STATEMENT**

The Constitution of the Republic of South Africa guarantees all persons or Data Subjects the right to privacy in the Bill of Rights. Therefore this right enjoys a high standard of protection by the highest law of the land in conjunction with other rights such as the right to dignity and the right to equality.

The POPIA is the vehicle through which the right to privacy and the enforcement of this right is being operationalized in the Republic of South Africa. POPIA governs the manner in which Personal and Special Personal Information is being processed, by setting conditions in line with international best practice, standards and principles that regulate the minimum requirements of lawful processing.

The AfroCentric Group is committed to protecting all Data Subjects’ privacy and ensuring that their Personal and Special Personal Information is used responsibly, ethically, appropriately, transparently, securely and in accordance with the applicable laws, in particular POPIA. The AfroCentric Group also recognises the significance that the rights to dignity and equality play in upholding all persons’ personal

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 3
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

information with confidentiality and ensuring that all processing is done with appropriate standards of security, without favour or bias.

The AfroCentric Group processes Personal and Special Personal Information about Data subjects as part of its business operations in the healthcare sector. The majority of the Group’s operations involve collecting, receiving, sharing, storing, transferring, aggregating Personal and Special Personal Information from different sources in order for the Group to service its clients, the ordinary beneficiaries of medical schemes, consumers of financial services and pharmaceutical goods and services and other equally important stakeholders. The AfroCentric Group has an integrated system of healthcare data, financial data, biometric data, unique identifiers and personal data from various sources which enables its business objectives. To this extent, the privacy of Data Subjects and consumers is critical in the success of the Group’s objectives.

The AfroCentric Group is committed to managing all Personal and Special Personal Information in an accountable, effective and efficient manner through the implementation of a POPIA Compliance Framework that takes into account a holistic and integrated, technical and organisational lawful processing of information objectives such as responsibly and orderly classification, retention and disposal of personal information, accessibility, security and confidentiality, training performance and quality management. The Group is committed to protecting records and documents that contain sensitive information of the company, customers, employees, suppliers and contractors.

### 3. POLICY OBJECTIVES

This Policy will:

- establish data retention standards and records management practices within the AfroCentric Group and align them with POPIA and all Applicable Data Protection Legislation:
- provide direction to the AfroCentric Group employees on the registration, creation, approval, receipt, access, organisation, storage, use and disposal of Personal and Special Personal Information that is held as Data.
- ensure that the AfroCentric Group is protected by complying with the POPIA and all Applicable Data Protection Legislation.
- ensure confidentiality, privacy, security, integrity, accessibility and retrievability of all the AfroCentric Group of all Data Subjects’ Personal and Special Personal Information to ensure the safety of all important and sensitive documents and information.
- establish a framework for classifying information based on its sensitivity, value and criticality to the Group in order to ensure that each category of information receives the kind of management and security it requires.
- set standards and periods for the retention of information within the Group, regardless of the business area or storage medium. The retention of any classified information shall be principally governed by the POPIA and the relevant subject–matter legislative requirements as shall be further set out in the retention schedule marked annexure A.

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 4
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

- Set methods and processes for the disposal and destruction of information that the Group no longer requires or where there is no longer a purpose for the information to be retained.
- provide for proper cleaning or destruction of sensitive/confidential data and licensed software on all computer systems, electronic devices and electronic media being disposed, recycled or transferred either as surplus property or to another user.
- Classification, retention and disposal processes of information is an integral part of the Group's overall data protection and security framework.

The Policy further ensures responsible and lawful access to Personal and Special Personal Information, as required by the AfroCentric Group. This will ensure efficient and effective execution of its functions. The policy further ensures continuity in the event of a disaster and protects the rights and interests of employees, clients, and other present and future stakeholders.

#### 4. SCOPE OF APPLICATION

This is a high level policy approved by the AfroCentric Group ("Group") to ensure a consistent approach to applying data privacy and security as prescribed by the POPIA, Applicable Data Protection Legislation as well as adherence to the principles of good corporate governance that are defined in the King IV Code <sup>TM</sup>.

Compliance with this Policy is required from and applicable to all the following Stakeholders that access or process all Personal data within **the Group**:

- the Group's directors and executive management, senior management, officers of the company, full time employee, part-time employees, and fixed term employees;
- independent consultants, and independent contractors;
- Beneficiaries of medical schemes, medical scheme clients and other clients of the Group;
- Third party service providers of the clients of the Group;
- Suppliers of services or goods to the Group; and
- users of the Group's infrastructure, information systems, networks and applications including those supplied under licence to Group.

The Policy applies to all data that belongs to the Group, our clients, our staff, our service providers and scheme members and beneficiaries.

All external parties that the AfroCentric Group shall share data with shall be (and are) legally bound by written data sharing agreements, or data processing agreements and the non-disclosure provisions applicable to them. Our Information Security Officer shall review all external parties' policies relevant to information security and records management to ensure that they are consistent with this policy.

It is the responsibility of all Group Stakeholders to adhere to the requirements detailed in this Policy and report any known or suspected violation of this Policy to the Group's Information Officer.

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 5
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

In this Policy, “AfroCentric”, “us”, “our” or “we” or “Group” or “AfroCentric Group” refers to one or more of the companies in the AfroCentric Group that operate in the Republic of South Africa. Whilst our subsidiaries generally use our systems and we have written agreements in place with them to comply with law, this Policy does not reflect the individual practices of our subsidiaries as they remain independent legal entities, however this policy represents the commitment to the protection of personal information, privacy rights and the standard required by the Group.

### 5. RELEVANT LEGISLATION

Other than Protection of Personal Information Act, 4 of 2013 that is the basis for this Policy, the AfroCentric Group also recognises and acknowledges the equal importance of the regulatory requirements of the following laws that protect the confidentiality and integrity of personal information:

- Children’s Act, 38 of 2005
- Companies Act, 71 of 2008
- Constitution of the Republic of South Africa, 1996
- Consumer Protection Act, 68 of 2008
- Cybercrimes Act, 19 of 2020
- Electronic Communications and Transactions Act, 25 of 2002
- Medical Schemes Act, 131 of 1998
- National Health Act, 61 of 2003
- Promotion of Access to Information Act, 2 of 2000
- Regulation of Interception of Communications and Provision of Communication-related Information Act, 70 of 2002
- King IV Report on Corporate Governance and the King IV Code, 2017 (King IV Code™)
- Financial Intelligence Centre Act, 38 of 2001
- Financial Advisory and Intermediary Services Act, 37 of 2002
- Financial Institutions (Protection of Funds) Act, 28 of 2001
- Financial Sector Regulation Act, 9 of 2017
- The South African Institute of Chartered Accountants: Guide on the Retention of Records
- Occupational Health and Safety Act, 1993 (OHS)
- Pension Funds Act, 1956
- Pharmacy Act, 1974
- Mental Health Care Act, 2002
- Medicines and Related Substances Act, 101 of 1965
- Hazardous Substances Act, 15 of 1973
- Insurance Act, 18 of 2017

This additional legislation shall also constitute Applicable Data Protection Legislation for the context of this Policy.

The AfroCentric Group encourages in all instances a robust culture of compliance with POPIA, Applicable Data Protection Legislation and this Policy in South Africa. Where there are subsidiaries operating outside of this country, the provisions of this Policy and the relevant provisions of such applicable data privacy and protection legislation shall take precedence over any governing company policy.

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 6
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

<b>6. RELATED POLICIES</b>	
<ul style="list-style-type: none"> <li>• Grievance Procedure</li> <li>• Human Capital Policies, Operational Risk Management Policy</li> <li>• Information Technology and Security Policies</li> <li>• Incident Management Policy</li> <li>• Clean Desk Policy</li> <li>• Legal Governance Policy</li> </ul>	
<b>7. DEFINITION OF TERMS</b>	
<b>TERM</b>	<b>DESCRIPTION</b>
<b>Responsible Party</b>	The legal entity that determines the purposes, methods and the use and processing of Personal Data, holds ultimate responsibility for implementing appropriate controls regarding the processing and for demonstrating its compliance with POPIA.
<b>Agreement(s)</b>	Legally executed agreement between any company of the AfroCentric Group and any Stakeholder along with annexures and any addendums as agreed between the Parties.
<b>AfroCentric Technologies (Proprietary) Limited or AfroTech</b>	A subsidiary of the AfroCentric Group which is primarily responsible for the establishment, maintenance and management of all information communications and technology based products and services within the Group.
<b>Crosscut shredding</b>	The process of destroying printed media by cutting it up both horizontally and vertically into small particles incapable of being reassembled
<b>Data</b>	Personal Information, Special Personal Information, Scheme Data, or any other information, whether 'structured' or 'unstructured', that is held in an electronic or any other format (including copies of data written or printed on paper, film, white boards or other media).
<b>Data Steward</b>	<p>A Data Steward is a technical IT professional operating within one of the knowledge areas, such as Data Integration Specialists, Database Administrators, Business Intelligence Specialists, Data Quality Analysts or Metadata Administrators.</p> <p>The Data Stewards are responsible for maintaining data on the IT infrastructure and ensure the safe custody, transfer, storage of the data and the implementation of business rules in line with the relevant data protection provisions contained in the POPI, all policies that specifically relate to security measures on the integrity and confidentiality of personal information and data.</p>
<b>Degaussing</b>	The process of creating a magnetic field close to magnetic storage media to destroy the data stored on the magnetic media, and which also destroys hard disk drives or fixed storage media beyond repair.
<b>Business Data Owner</b>	<p>The Business Data Owner is an Executive Manager of the company that is an accountable person who will oversee and protect the utilisation of data within their respective business unit or division.</p> <p>Business Data Owners are business professionals, most often recognized subject matter experts, accountable for a subset of data.</p>

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 7
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

	They work with the Information Office and the Data Stewards to define and control data.
<b>Electronic Storage Media</b>	Any device, component or mechanism that can electronically store and give access to any data, for example, CD-ROM disks, PC hard drives, removable storage such as USB flash disks, magnetic tapes and so on.
<b>Data Subject</b>	<p>Any natural or juristic person who is identifiable by means of an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity.</p> <p>In the context of this Policy this is the person (also known as customer) whose Personal and Special Personal Information is being processed by the AfroCentric Group.</p>
<b>Employees/Personnel</b>	Individuals employed by the Group under a permanent, part-time or fixed term employment contract including temporary staff who are employed by employment agencies that are contracted to the Group.
<b>DPR</b>	The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information from individuals who live in the European Union (EU).
<b>POPIA</b>	The Protection of Personal Information Act 4 of 2013 (POPIA) is the comprehensive data protection legislation enacted in South Africa. POPIA aims to give effect to the constitutional right to privacy, whilst balancing this against competing rights and interests, particularly the right of access to information.
<b>Personal Information</b>	<p>Any information relating to an identified or identifiable person, natural or juristic ('Data Subject');</p> <p>an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</p>
<b>Processing or Process</b>	Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information including collection, receipt, updating, recording, organisation, collation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination by means of transmission or otherwise making available in any other form, alignment or combination, erasure or destruction of Personal Information, merging or linking, as well as restriction, degradation.
<b>Special personal information</b>	Information concerning a child and personal information concerning the religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, DNA, sexual life or criminal behaviour of a Data Subject.
<b>Stakeholder or Group Stakeholder</b>	A variety of Data Subjects with vested interest and rights to the processing of their Personal and Special Personal Information by the AfroCentric Group and shall include without limitation, employees, shareholders, business partners, clients, service providers, customers, beneficiaries of medical schemes, suppliers and any other identifiable

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 8
Review Date:	31 August 2023	



## GROUP DATA PRIVACY POLICY

	<p>person with whom the Group has business relations which involve the processing of Personal and Special Personal Information.</p>
<b>Operator</b>	<p>The party who processes (collect, receive, record, collate, store, anonymise, retrieve, alter, use, distribute, erase or delete) information for a responsible party in terms of a contractual agreement or mandate on behalf of a Responsible Party.</p> <p>In the context of this policy this is either the AfroCentric Group or a business partner.</p>
<b>Scheme Data</b>	<p>All details and information relating to the medical scheme clients of the Groups and their members including (without limitation):</p> <ul style="list-style-type: none"> <li>• The Scheme’s own financial, statistical, human resources or other data which is generated by the Scheme or Medscheme pursuant to rendering the administration services, or required by the Scheme for its ordinary operations, or as may be obtained from third parties for purposes of processing claims or otherwise rendering services to members;</li> <li>• information relating to the members’ or beneficiaries’ medical records;</li> <li>• personal details of members and beneficiaries;</li> <li>• lists of members and beneficiaries;</li> <li>• claims made by beneficiaries (including the physical claims);</li> <li>• benefits paid to members;</li> <li>• Scheme service provider information;</li> <li>• financial, statistical and other data related to the business of the Scheme and its members; and</li> <li>• minutes of meetings of the Scheme, be it Board of Trustee meetings or any other types of meetings;</li> </ul>
<b>Responsible Party</b>	<p>The party who determines the purpose of and means for processing personal information and is also responsible for protecting (safeguarding) the information of the Data Subject.</p> <p>In the context of this policy this is either the AfroCentric Group or a business partner (depending on the context).</p>

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 9
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

<b>Information Regulator</b>	The Information Regulator Office duties shall include providing education, monitor and enforce compliance, handle complaints and facilitate cross-border cooperation in the enforcement of privacy laws. In the context of this Statement this is the office of individuals appointed by the President of South Africa in terms of POPIA.
<b>Information Officer “IO”</b>	The Chief Executive Officer of the AfroCentric Group or such other individual appointed by the Chief Executive Officer in his stead who is registered with the Information Regulator in terms of the PAIA and POPIA and is responsible for ensuring that the AfroCentric Group complies with the aforementioned Acts.
<b>IP</b>	any intellectual property of the Group, including but, not limited to software, code, documentation, schematic, intranet content, website content, design, drawing, logo, database, copyrighted work, trade mark, patent, email, voice mail or fax.
<b>IT Assets</b>	Any IT equipment capable of storing data, such as PCs, servers, electronic storage media and portable devices.
<b>Structured data</b>	Data that is usually centrally stored, catalogued, indexed and managed by technology in a way that allows querying and reporting against predetermined data types and understood relationships, for example the Oracle Financials, Oracle HR and Nexus databases.
<b>Unstructured Data</b>	Data that is not centrally stored and managed, but is widely distributed and managed locally by individual data users and usually consists of either: (1) non-language based data such as image, video or audio files, and (2) textual data such as Microsoft Word documents, e-mails or Excel spreadsheets.
<b>Physical Destruction</b>	The process of physically destroying storage media to permanently prevent any future access to stored data, including crushing, heating and crosscut shredding, or the process of physically erasing data on media such as white boards
<b>Printed Media</b>	Copies of data written or printed on any form of media such as paper, cardboard, flip charts, film or whiteboards and expressly includes handwritten notes
<b>Supervisory Authority</b>	Information Regulator (IR)
<b>Wipe</b>	To delete data and then overwrite that disk space at least five times with random character.
<b>Group</b>	AfroCentric Group and its subsidiaries

### 8. POLICY PROVISIONS

#### GROUP ROLES AND RESPONSIBILITIES

All managers, executives and employees of Afrocentric Group shall ensure that:

- The provision of this policy are read, understood and adhered to.

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 10
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

ROLE	DESCRIPTION
<b>The Board</b>	<p><b>The Board.</b></p> <ul style="list-style-type: none"> <li>Is ultimately responsible for corporate governance and compliance with applicable rules and regulations including Group data privacy policy.</li> </ul>
<b>Audit &amp; Risk Committee</b>	<p><b>The Audit &amp; Risk Committee:</b></p> <ul style="list-style-type: none"> <li>Responsible for overseeing the roles and responsibilities of the Internal Audit team, specifically relating to providing assurance in respect of Enterprise Risk Management</li> </ul>
<b>Group CEO</b>	<p><b>Group CEO:</b></p> <ul style="list-style-type: none"> <li>Sets the tone at the top that influences the Compliance Culture and other components of Enterprise Risk Management within the Group.</li> </ul>
<b>Compliance Function</b>	<p><b>The Compliance Function:</b></p> <ul style="list-style-type: none"> <li>Reviews and ensure the approval of the Regulatory Universe.</li> <li>Assists with the effective management of compliance risk in the Group.</li> <li>Assists management in discharging their responsibility to comply with applicable legislation &amp; regulatory requirements.</li> <li>Assists with the implementation of the compliance risk management process through the identification, assessment, management, monitoring and reporting of Compliance Risks that are faced by the Group.</li> <li>Reports all instances of non-compliance with regulatory requirements to the governing bodies.</li> </ul>
<b>Executive Enterprise Risk Management Committee(EERCO)</b>	<p><b>EERCO:</b></p> <ul style="list-style-type: none"> <li>Addresses the corporate governance requirements and monitors the Group's performance against any identified risk.</li> </ul>
<b>Business Unit / Divisional Enterprise Risk Management Committees</b>	<p><b>Business Unit / Divisional Enterprise Risk Management Committees:</b></p> <ul style="list-style-type: none"> <li>Implement Enterprise Risk Management methodologies and processes in line with the AfroCentric Group Enterprise Risk Management Framework.</li> <li>Identify, evaluate and review specific compliance risks, assessing their impact and probability, assigning owners and defining actions to address these risks.</li> <li>Report any significant Compliance Risks that could have a direct or indirect impact on the operational objectives to the Compliance Function.</li> </ul>
<b>BU Management</b>	<p><b>Management:</b></p> <ul style="list-style-type: none"> <li>Conducts all business in compliance with the applicable legislation and regulatory requirements.</li> <li>Enforces necessary measures and controls to ensure that this policy is adhered to at all times within the business.</li> </ul>

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 11
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

	<ul style="list-style-type: none"> <li>• Takes the necessary and appropriate disciplinary action against an employee who is in breach of the terms of this policy.</li> </ul>
<b>Employees</b>	<b>Employees:</b> <ul style="list-style-type: none"> <li>• Ensure that the provisions of this policy are read and understood.</li> <li>• Ensure adherence to this policy.</li> <li>• Implement the specific Regulatory Requirements applicable to their day-to-day activities.</li> </ul>
<b>Internal Audit</b>	<b>Internal Audit:</b> <ul style="list-style-type: none"> <li>• Provides assurance that management processes are adequate to identify and monitor significant compliance risks.</li> <li>• Assesses the adequacy and effectiveness of the Compliance Function in accordance with the Internal Audit plan as approved by the Risk Management and Audit Committees and/or as required.</li> </ul>

### 8.1 ROLES

- **AFROCENTRIC GROUP AS A RESPONSIBLE PARTY**

As a Responsible Party, the AfroCentric Group is empowered to decide:

- to collect the personal information in the first place and the legal basis for doing so.
- which personal information to collect.
- the purpose(s) the information are to be used for.
- which individuals to collect information about.
- whether to disclose the information, and if so, who to.
- whether subject access and other individuals' rights apply.
- how long to retain the information or whether to make non-routine amendments to the information.

To the extent that the AfroCentric Group collects Personal Information of customers, clients, site visitors, and other targets to sell goods and services other than medical scheme related services, it must do so on the basis of lawful and legitimate purpose. The AfroCentric Group has an embedded Code of Conduct and the Code of Ethics that require all employees of the Group to respect the confidentiality of information acquired as a result of their professional, business and contractual relationships.

Employees must not disclose any confidential information to third parties unless there is a legal or professional right or duty to disclose and /or written authority has been obtained to disclose such information. Employees of the Group must not use any personal information to their advantage.

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 12
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

AfroCentric Group is committed to conducting business ethically and with integrity in accordance to the POPIA and applicable Data Protection Legislation. It shall ensure that it processes all personal information within the parameters of the agreements and mandates it has put in place, honestly and with transparency.

- **THE AFROCENTRIC GROUP AS AN OPERATOR**

As an Operator, AfroCentric Group acts on the mandates and legally valid written agreements of its clients, who are responsible parties. These agreements clearly indicate that personal information is owned by or belongs to the customers or beneficiaries of the client and as such, the AfroCentric Group may not process such information beyond the scope of the services that it is appointed to provide.

The Group does not assume the role of the Responsible Party over the personal information that is disclosed to it (especially Scheme Data) by its clients for the purposes of providing medical scheme administration services or managed healthcare services and/or other specified services. The Group carries out the actual processing of the personal information under specific instructions of the data controller.

The role of the Group as the Operator is limited to the following:

- the design, creation, and implementation of information and communications technology and related processes and systems that enable Responsible Party to gather personal information.
- the usage of tools and strategies to gather personal information.
- implementation of security measures that safeguard personal information.
- storage of personal information gathered by the Responsible Party.
- the means used to transfer the personal information from one company to another.
- the means used to retrieve personal information about certain Data Subjects.
- the method for ensuring a retention schedule is adhered to.
- the means used to delete or dispose of the information.

The duty to prove compliance with the privacy obligations is on the Responsible Party to whom the AfroCentric Group reports to. In this context the AfroCentric Group shall only fulfil the role of an Operator in accordance with its mandate.

### 8.2 POLICY PRINCIPLES

#### PART I - AFROCENTRIC GROUP'S RESPONSIBILITIES AS A RESPONSIBLE PARTY

The following principles will apply to the AfroCentric Group as a Responsible Party, it will:

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 13
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

- comply with POPIA and the Data Protection Legislation and follow generally accepted information practices such as standards issued by the ISO.
- comply with all the conditions for lawful processing of personal and/or special personal information applicable to it, in its capacity as a responsible party.
- protect the rights of Data Subjects such as employees, service providers, consultants, third parties and clients whose personal and/or special personal information the Group processes.
- be transparent towards all Data Subjects whose information it processes and notify them on how the Group processes or intends to process those Data Subjects' personal and/or special personal information; and
- monitor, identify, protect, investigate, remediate and communicate the risks involved with all security compromises or breaches of personal and/or special personal information.

This part of the policy excludes any processing related to the services that the Group provides to medical scheme clients and other third party clients to whom we are bound by the scope of the mandates. This is dealt with where the Group assumes the role of an Operator.

The Group is a Responsible Party for the following functional areas and it will implement the privacy controls to safeguard the personal information it processes:

**Human Capital (HC):** Collects personal information on job applicants and **employees** to comply with laws (Basic Conditions of Employment Act, Employment Equity Act), assisting the Company with the selection of employees for employment, training, promotions, ensuring safety at the workplace, quality control, customer service, and the protection of both the employee and the employer's property. HC also determines the means of processing related to payroll services, which include pay as you earn, unemployment insurance contributions, Group risk benefits, employee development planning and review, performance appraisals, training, business travel expense and tuition reimbursement, identification cards, access to the Group's facilities and ICT, employee profiles, internal employee directories, record keeping, and other employment related purposes.

**Finance:** Processes personal information related to budgets and general finances, procurement and creditors, insurance for the AfroCentric Group, facilitating payments and receiving banking details from service providers, manage banking log-in details, updating of vendor personal details and other sensitive information related to the financials of the Group such as annual financial statements. It also engages with and provides details to the Compensation Commissioner related to the Group's Compensation for Occupational Injuries and Diseases act registration.

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 14
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

**Communications and Stakeholder Engagement:** Processes general information on all stakeholders that the Group has identified as part of the stakeholder matrix and communicates information regarding the Group and other stakeholders to these stakeholders. Occasionally the Group also processes information of customers, business partners, vendors, service partners and suppliers to complete surveys that are used for marketing and quality assurance purposes.

**Corporate:** Gains first hand knowledge into handling and managing of key business accounts which is paramount to the Group' business development and value realisation objectives. Part of this includes direct engagement with directors of the Group where strategic decisions around the operating of the Group is made. This reference is related to matters of structuring the business including managing the finances in a prudent manner.

**Technology:** To implement internal security controls to protect personal information of the Group, including information of employees, services providers and other related company information as prescribed above and adding processes and controls that support privacy principles.

**Privacy, Legal and Compliance:** To Identify privacy **obligations** for the Group; identify business, employee and customer privacy risks; identify existing documentation, policies and procedures; create, revise and implement policies and procedures that effect positive practices and together that comprise a privacy program's scope and purpose. Processing that takes place are internal documents that are not appropriate for external sharing and usage. This functional area also processes information such as contracts and due diligence documents of third-party service providers.

In its capacity as the Responsible Party, the Afrocentric Group subscribes and binds itself to the following principles:

- **Accountability:** Adhere to the 8 (eight) processing conditions set out in POPIA, as per the bullets below.
- **Purpose Limitation:** Only process the Personal Data with the appropriate legal justification such as:
  - With consent of the Data Subject – consent must be obtained for any new purpose of processing (new engagement/interaction with a Data Subject) or in respect of any

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 15
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

processing that is different or no longer compatible with the initial purpose that the Data Subject is aware of. The Group's Consent Standards must be adhered to in this regard.

- legitimate interest of the Data Subject;
  - conclusion or performance of a contract;
  - compliance with an obligation in law; and,
  - collection of the personal information directly from the Data Subjects, unless exception to collecting it directly from the Data Subjects apply.
- **Purpose Specification:** Only collect the information for a specific, explicitly defined and lawful purpose. The Group will also only retain the information while it has a legitimate business purpose of which the Data Subject is made aware, unless prescribed otherwise by law. Where it may no longer retain the information, it will destroy or delete records of personal information in a manner that prevents it from being re-identified.
  - **Processing of personal information for a secondary purpose:** The Group will not process information for a secondary purpose, unless the processing is compatible with the initial purpose the information was collected for, or the Group obtained consent to process the information for a different purpose have been obtained from the Data Subject.
  - **Information Quality:** The Group will take all reasonably practicable steps to ensure that personal information it collects and/or processes are complete, accurate, not misleading and updated where necessary, considering the purpose for which such information is initially collected.
  - **Openness and Transparency:** The Group will take all reasonably practicable steps to ensure that the Data Subject is aware of the purpose and processing activities of the personal information it processes.
  - **Security measures:** The Group will secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to, or unauthorised destruction of personal information, and unlawful access to or processing of personal information.
  - **Data Subject Rights and Participation:** The Group will allow Data Subjects to exercise their rights to request to confirm, free of charge, whether the Group holds personal information about the Data Subject.

The Group will allow Data Subjects to exercise their rights to request a company to correct or delete personal information about the Data Subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.

It will furthermore allow Data Subjects to request that their information be destroyed or deleted if the Group is no longer authorised to retain the information in terms of any legislation or regulation.

The Group will afford Data Subjects an opportunity to object, on reasonable grounds relating to his, her or its particular situation to the processing of his, her or its personal information, if such processing is based on a legal justification to process such information.

### Data Privacy Breaches

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 16
Review Date:	31 August 2023	



## **GROUP DATA PRIVACY POLICY**

The Group will immediately or as soon as reasonably possible after the discovery of a security compromise which impacts a Data Subject, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the affected party's information system, notify the Data Subject and Information Regulator thereof.

When a security compromise of Personal Data is identified, the Group's Incident Management Policy shall be complied with to ensure expeditious and effective response to such an incident.

### **Confidentiality and security obligations in Agreements**

The Group shall ensure that individuals operating under its control with access to Personal Data are subject to a confidentiality obligation. All agreements to be concluded by or on behalf of the Group with Operators shall set out confidentiality obligations of the parties, purpose specification and limitation and require such Operators to take responsibility of maintaining the integrity and confidentiality of Personal Data in their possession or under their control by taking appropriate, reasonable technical and organisational measures to prevent loss of, damage to, or unauthorised destruction of personal information, and unlawful access to or processing of personal information. These agreements should specify the length of time the obligations should be adhered to. The Legal Governance Policy of the Group must be implemented to realise this requirement.

### **Processing of Special Personal Information**

The Group shall adhere to the following principles when it processes **special personal information and will only process Special Personal Information if:**

- the Information Regulator (IR) has authorised such processing.
- processing is carried out with the consent of a Data Subject.
- processing is necessary for the establishment, exercise or defence of a right or obligation in law.
- processing is necessary to comply with an obligation of international public law.
- processing is for historical, statistical or research purposes to the extent that the purpose serves a public interest and the processing is necessary for the purpose concerned;
- 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
- information has deliberately been made public by the Data Subject.

### **Cross-Border Sharing Of Personal Information**

The Group will not transfer personal information about a Data Subject to a third party who is in a foreign country unless:

- the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection;
- the Data Subject consents to the transfer;
- 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;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Group and a third party;
- the transfer is for the benefit of the Data Subject;
- it is not reasonably practicable to obtain the consent of the Data Subject to that transfer; and

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 17
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

- if it were reasonably practicable to obtain such consent, the Data Subject would be likely to give it.

### **Automated decision making/Profiling:**

- The Group will not subject a Data Subject to a decision which results in legal consequences for him, her or it, which is based solely on the basis of the automated processing of personal information (without human intervention) intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences or conduct.
- If it does, it will:
  - provide an opportunity for the Data Subject to make representations about a decision; and
  - provide the Data Subject with sufficient information about the underlying logic of the automated processing of the information relating to him or her to enable him or her to make the necessary representations.

### **Direct Marketing:**

- AfroCentric Group shall not engage in direct-marketing unless the following requirements are complied with:
  - the Data Subject has consented or the processing falls within the scope of one of the other lawful bases for the processing of personal information; or,
  - the Data Subject is a customer of the Group and;
    - the Group has obtained the details of the Data Subject in the context of the sale of a product or service that is sold by the Group;
    - for the purpose of direct marketing the Group's own similar products or services; and
    - the Data Subject has not objected to this processing despite having had a reasonable opportunity to object, free of charge, without the necessity of formality, at the time when the information was collected and when each communication is sent to the Data Subject for this purpose.
  - the direct marketing communication contains details of the identity of the direct marketer or the person on whose behalf the communication has been sent (section 69(4) of POPIA); and
  - the direct marketing communication contains an address or other contact details to which the relevant Data Subject (consumer) may send an objection to the processing of their personal information.
- The Group's marketing strategy also includes a business to business model. As such it may approach other companies to participate in its business initiatives or collaborate with any of its

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 18
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

entities to realise shared value objectives after implementation thereof. POPIA expands the definition of personal information to include identifiable information of juristic entities.

- Considering the above, the Group will allow these businesses to object, at any time, to the processing of personal information for purposes of direct marketing other than direct marketing by means of unsolicited electronic communications (telephonic, in person or post). If a Data Subject objects to the processing of personal information, the request must be honoured, and the personal information of the Data Subject may no longer be processed for direct marketing purposes.
- The Group will also not process the personal information of these businesses for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines (i.e. machines that are able to do automated calls without human intervention), facsimile machines, SMSs or e-mail, push notifications on social media platforms, unless these businesses:
  - have given their consent to the processing; or,
  - is a customer of the Group who has not previously objected to such marketing.
- Excluded from these requirements are instances where the Group may generally advertise its services and these advertisements are not targeted at a specific business or customer.

### **Information Security**

- The Group emphasises adherence to the Information Security Policy for all its staff and relevant stakeholders in line with its objective to align current processes with POPIA.
- Employee Training on Cyber Security and Data Privacy forms part of ongoing compliance training of the AfroCentric Group. Cyber Security training is currently further required as a basic compliance training that all employees must complete. As part of the POPIA management programme, there is a specific focus on training, awareness as well as communication that will cover data privacy, data security and more detailed cyber security training as mandatory compliance training to all staff.

## **PART II - AFROCENTRIC GROUP RESPONSIBILITY AS AN OPERATOR**

The AfroCentric Group values the trust and good faith principles that are the cornerstone of its numerous relationships with its clients. The Group is committed to maintaining the relationships it has established and has yet to establish with its various stakeholders and to conduct business ethically and honestly even when it manages the personal information and data that it is entrusted with to be able to conduct its business operations.

As an Operator, the Group shall comply with the following principles:

- It and its representatives will only process personal information on behalf of the client medical schemes, financial services institutions, medical scheme beneficiaries, third party service providers, business partners, customers of its various goods and services with their prior written knowledge and authorisation. This is despite the authorisation being afforded in general terms in terms of the valid and enforceable array of legal Agreements.

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 19
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

- At all times treat personal information which comes to its knowledge as confidential and will not disclose it, unless required by law or during the proper performance of their contractual duties, pursuant to the Agreements and any other agreements placing obligations on the Group.
- Where there are reasonable grounds to believe that the personal information of a Data Subject has been accessed or acquired by any unauthorised person, the Group will initiate investigation and immediately notify the stakeholders whose Data Subject(s) information were potentially compromised of such a compromise.
- Provide sufficient guarantees to the stakeholders that it will implement appropriate, reasonable, technical and organisational measures to ensure the lawful processing and the protection of the Data Subjects' rights. This includes insofar as this is possible, assisting in the fulfilment of the stakeholders' obligation to respond to Data Subject requests.
- Will not engage another Operator without prior specific or general written authorisation from the stakeholders.
- Inform the stakeholders of any intended changes to add or replace existing sub-Operators and give them an opportunity to object to such changes.
- Ensure that representatives of the stakeholders processing the personal information of the stakeholders for the purpose of the services and good that are being performed by the Group, commit themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- Where possible and required, assist the stakeholders in ensuring compliance with the following obligations:
  - Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of processing data for purpose related to the services and goods.
  - Notify the stakeholders without undue delay after becoming aware of a personal data breach.
- If the breach occurred while the information was under the control of the Group, it will provide all the required information of the breach to the stakeholders. The information required will include the nature of the personal data breach, contact point where the information may be obtained, likely consequences of the breach and the measure or proposed measures to be taken to avoid adverse effects to the Data Subjects.
- Assist the stakeholders with details required to, where required, to conduct a data protection impact assessment.

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 20
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

- On request of the stakeholders, the Group will delete or return all the personal information after the end of the services provided by the Group to the stakeholders subject to the Group being able to do so without breaching its other lawful obligations.
- Make evidence and information available to the stakeholders to enable the stakeholders to prove their compliance with the conditions/principles for lawful processing, specifically those imposed on the stakeholders in respect of Operators.
- The Group will immediately inform the stakeholders if in its view, an instruction is a transgression of any condition/principles prescribed by privacy law.
- Ensure that the same obligations that the Group must meet in its capacity as Operator, are imposed on sub-Operators that the Group engages with.
- The Group will not during any engagement with the stakeholders related to the performance of the services and goods, determine the means or purpose of processing for its stakeholders which are Responsible Parties.
- The Group will implement and certify itself in accordance with the information security and data privacy frameworks to ensure that the stakeholders can prove its Operator complies with the privacy obligations imposed on the stakeholders as responsible parties.
- The Group, its employees and business partners have agreed that no personal information shall be sold, rented or provided to unauthorised entities or other third parties for their independent use, without the consent of the Data Subject.
- Contractual Obligations

To ensure adherence to the Policy principles and the requirements applicable to Operators, the Group holds itself accountable to the various contractual obligations, duties and responsibilities that it has concluded with its clients.

The contracts record detailed data protection and usage obligations between the parties for purposes stated in those individual contracts.

The core business activities of the Group are medical scheme administration services and managed healthcare services. Through its ability to offer these services to mainly medical schemes in South Africa, the Group has access to the personal and special personal information of all beneficiaries of medical aid provided by its medical scheme clients. To this extent, the Group once again recognises the great significance of protecting the privacy of the personal and special personal information. The Group, in particular its directly appointed subsidiaries, shall only process personal and special personal information for the following purposes:

**A. Accredited Administration Services including but not limited to:**

- Membership Record Management - verification of members, processing of new applications, registration of membership, management of contributions;

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 21
Review Date:	31 August 2023	

## **GROUP DATA PRIVACY POLICY**

- Contribution Management;
- Financial Management;
- Claims Management;
- Customer Services;
- Broker Remuneration and Management;
- Information Management and Data Control, and;
- Other services that may otherwise be added by the regulatory authorities under this scope of services is otherwise contracted to provide to medical schemes.

**B. Supplementary Administration Services including but not limited to:**

- Actuarial Services;
- Benefit Management services;
- Distribution Services;
- Internal Audit Services;
- Broker services;
- Marketing services;
- Third party recovery services;
- Forensic investigations and recoveries;
- Governance and Compliance Services;
- Optometry Management services, and;
- Other services that may otherwise be added by the regulatory authorities under scope of services which the Group is otherwise contracted to provide to medical schemes.

**C. Managed healthcare services including but not limited to:**

- Hospital Benefit Management;
- Pharmacy Benefit Management;
- Disease Management;
- Network Management;
- Dental Management, and;
- Other services that may otherwise be added by the regulatory authorities under scope of services which the Group is otherwise contracted to provide to medical schemes.

**D. Other services including but not limited to:**

- Marketing and branding services;
- Financial services relating to the sale and provision of financial products and services;
- Information Communications and Technology services;
- The manufacturing, wholesaling and distribution of health products intended for human and animal use;
- The retail sale and distribution of pharmaceutical health products and devices;
- Medical prescriptions and the delivery of pharmaceutical health products; and/or
- Any other service which the Group is bound in terms of a lawful and enforceable Agreement to perform.

**PART III - EMPLOYEE TRAINING ON CYBER SECURITY AND DATA PRIVACY**

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 22
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

The Group's employees are bound to attend to the following ongoing training obligations:

- Cyber Security Online Training
- POPIA Online Training and Data Privacy forms part of ongoing compliance training of the Group.

There shall be specific focus on training, awareness as well as communication that will cover data privacy, data security and more detailed cyber security training.

### **PART IV - DISPOSAL OF DATA**

Where it may no longer retain the information, the Group will destroy or delete records of data, personal or special personal information in a manner that prevents it from being re-identified.

The Group shall allow a Data Subject to exercise its right to request a relevant subsidiary of the Group to correct or delete personal information about the Data Subject if it is misleading or obtained unlawfully.

No person shall archive, destroy or erase or otherwise dispose of or archive any Data or special personal information stored in any format as a record (including e-mail) may be without prior written request or approval of the Information Officer or Executive Manager or such other of a duly authorised person or officer of the Group who is responsible for the management of data privacy and/or security.

When the Business Data Owner together with Information Officer and Information Security Officer approve the archiving, destruction, erasure or otherwise disposal of a record of personal information or special personal information, this approval must be made with due regard to the Retention Periods as indicated in Annexure A of this Policy.

In execution of any instruction relating to disposal, all personnel must ensure that no archival records are inadvertently destroyed.

The Legal department must always be consulted before any disposal or destruction or erasure is executed.

Any data, personal or special personal information (in a manner) that has one or more characteristics listed below qualifies to be deleted, that is if it is:

- no longer required to be retained in accordance with the Retention Periods listed in Annexure A;
- no longer required for the purpose for which it was initially collected and it is also not subject to any legal retention requirements;
- pursuant to a termination of an agreement with a third party and the Group is no longer required to retain a copy of that data by any law or statutory authority;
- it is irrelevant to the business of the Group or the requirements of the Data Subject or any stakeholder; or
- incorrect,

The destruction of records or data should render such data or record non-recoverable by any means.

Data must be destroyed in the following ways:

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 23
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

Data Classification	Data Type	Discard	Shredding bins	Crosscut shredding	Delete	Delete and wipe	Degauss	Physically destroy
<b>Public</b>	Printed Media (including hand written notes)	✓						
	Electronic storage media (excluding Flash disks)	✓						
	Flash memory disks				✓			
<b>Internal</b>  (company confidential)	Printed Media (including hand written notes)		✓					
	Electronic storage media (excluding Flash disks)				✓			
	Flash memory disks				✓			
<b>Restricted</b>  (company secret)	Printed Media (including hand written notes)			✓				✓
	Electronic storage media (excluding Flash disks)					✓		
	Flash memory disks					✓		
<b>Top secret</b>  (highly sensitive)	Printed Media (including hand written notes)			✓				✓
	Electronic storage media (excluding Flash disks)						✓	

Policy:	Group Data Privacy Policy		
Custodian:	Group Chief Financial Officer: Compliance		
Approval Date:	September 2021	Version No. 1.0	
Implementation Date:	September 2021	Page: 24	
Review Date:	31 August 2023		



## GROUP DATA PRIVACY POLICY

	Flash memory disks							✓
--	--------------------	--	--	--	--	--	--	---

Records that are not archived which are needed for purposes of litigation, promotion of administrative justice actions and promotion of access to information purposes may not be disposed of until such time that the Information Officer together with Information Security Officer and the relevant Business Data Owner responsible for records Management, in consultation with the Legal Department, have indicated in writing that the destruction hold can be lifted.

This covers every kind of personal information and/or special personal information processed or stored in any way within our Group. It applies to all personal information and/or special personal information that belongs to the Stakeholders as defined:

- 

All external parties that we share personal information or special personal information with, shall be legally bound by written data protection and reciprocal non-disclosure agreements, which include data retention provisions where relevant.

The Group’s Business Data Owners and the Information Security Officer shall reviews external parties’ policies relevant to information security and records management to ensure that they are consistent with this Policy.

### PART V - CLASSIFICATON OF DATA

All data documented or stored in or created within the Group must be classified or declassified by the Information Officer together with the Executive Manager responsible for Information Communications and Technology in the Group.

This section of the Policy defines the types of Data that must be classified and specify who is responsible for data classification, protection and handling. As either the Responsible Party or an Operator, the Group is entrusted to deal with the following classes of information:

- **Restricted / Sensitive Information:** information that must be protected from unauthorised access or disclosure which forms an integral of private rights of the Group and its stakeholders. If this information is disclosed to the unauthorised third parties or the public, it will cause a great embarrassment, cause an inconvenience to the business or lives, bring disrepute or threaten the sustainability or reputation of the Group and its stakeholders.
- **Confidential Information:** any information of whatever nature, which has been or may be obtained by the Group from its stakeholders, whether in writing or in electronic form, or pursuant to discussions between the Group and its stakeholders, or which can be obtained by examination, testing, visual inspection or analyses, including, without limitation, scientific, business or financial data, know-how, formulae, processes, designs, sketches, photographs, plans, drawings, specifications, sample reports, models, customer lists, price lists, studies, findings, computer software, inventions or ideas; analyses, concepts, compilations, studies and other material prepared by or in possession or control of the recipient which contain or otherwise reflect or are generated from any such information as is specified in this definition;
- **Secret / Classified Information:** Confidential Information that only a select few personnel of the

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 25
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

Group are authorised to access. Secret information is subject to access control and management measures. Classified information is any information that is governed by law or regulation.

- **Personal Information:** as defined in item 7 of this Policy. This information is regulated by POPIA in South Africa or the GDPR. This information can be categorized as Restricted/Sensitive Information as well and is regulated by POPIA in South Africa or the GDPR.
- **Special Personal Information:** as defined in item 7 of this Policy. This information can be categorized as Restricted/Sensitive Information as well and is regulated by POPIA in South Africa or the GDPR.
- **Other:** any such information that is otherwise deemed confidential, restricted or sensitive or secret by the Executive Managers or the Information Officer which has the potential to cause harm if disclosed without prior written authority or consent.

All the categories of Classified Information must be observed in all business activities of the Group by ensuring that the confidentiality, integrity and security of this Classified Information is not violated and interfered with.

The above categories determine the scope of processing for the different categories of the Classified Information.

Each company in the Group is required to designate personnel who will be responsible for carrying out the duties associated with each of the roles set out hereunder:

Role	Description of Role and Responsibilities
<b>Data Owner</b>	<p>Responsible for the data and information being collected and maintained by his or her department or division, usually a member of senior management.</p> <p>The Business Data Owner shall be responsible for:</p> <ol style="list-style-type: none"> <li>1. <b>Review and categorization</b> - Review and categorize data and information collected by his or her company or business unit</li> <li>2. <b>Assignment of data classification labels</b> - Assign data classification labels based on the data's potential impact level</li> <li>3. <b>Data compilation</b> - Ensure that data compiled from multiple sources is classified with at least the most secure classification level of any individually classified data</li> <li>4. <b>Data classification coordination</b> - Ensure that data shared between departments is consistently classified and protected</li> <li>5. <b>Data classification compliance</b> - Ensure that information with high and moderate impact level is secured in accordance with federal or state regulations and guidelines</li> <li>6. <b>Data access</b> - Develop data access guidelines for each data</li> </ol>

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 26
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

	<p style="text-align: center;">classification label.</p> <p>Business Data Owners shall also ensure that they assist the Information Office with the identification of records which must be corrected, disposed of or archived taking into consideration the principles of data protection contained in the Groups Data Privacy Policy.</p>	
<p><b>Data Stewards</b></p>	<p>The Data Stewards are responsible for maintaining data on the IT infrastructure and ensure the safe custody, transfer, storage of the data and the implementation of business rules in line with the relevant data protection provisions contained in the POPI, all policies that specifically relate to security measures on the integrity and confidentiality of personal information and data.</p> <p>They shall be responsible for maintaining and backing up the systems, databases and servers that store the organisation’s data. This role shall also ensure that there is a technical deployment of all the rules set forth by the Information Privacy Office and the Business Data Owners and that the rules applied within system are functional.</p> <p>The Data Stewards role will be sub-categorised as follows:</p> <ul style="list-style-type: none"> <li>• Executive Data Stewards are senior managers or general managers who serve on a Data Governance Council;</li> <li>• Enterprise Data Stewards shall have oversight of a data domain across the AfroCentric Group;</li> </ul> <p>The Data Stewards must:</p> <ol style="list-style-type: none"> <li>1. <b>Access Control</b> - Ensure that proper access controls are implemented, monitored and audited in accordance with the data classification labels assigned by the Business Data Owner;</li> <li>2. <b>Audit reports</b> - Submit an annual report to the Business Data Owners that addresses availability, integrity and confidentiality of classified data;</li> <li>3. <b>Data backups</b> - Perform regular backups of all AfroCentric Group data within their allocated business areas ;</li> <li>4. <b>Data validation</b> - Periodically validate data integrity;</li> <li>5. <b>Data restoration</b> - Restore data from backup media;</li> <li>6. <b>Compliance</b> - Fulfill the data requirements specified in the AfroCentric Group’s security policies, standards and guidelines pertaining to information security and data protection;</li> <li>7. <b>Monitor activity</b> - Monitor and record data activity, including information on who accessed what data;</li> <li>8. <b>Secure storage</b> — Encrypt sensitive data at rest while in storage;</li> </ol>	

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 27
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

audit storage area network (SAN) administrator activity and review access logs regularly;

9. **Data classification compliance (in conjunction with data owners)** — Ensure that information with high and moderate impact level is secured in accordance with POPIA and Applicable Data Protection Legislation;
10. **Data access (in conjunction with data owners)** — Develop data access guidelines for each data classification label;
11. **Create and manage core Metadata:** Definition and management of business terminology, valid data values, and other critical Metadata. Stewards must design and formulate the AfroCentric Business Glossary, which becomes the system of record for business terms related to data.
12. **Document rules and standards:** Stewards will be responsible for the definition/documentation of business rules, data standards, and data quality rules. Expectations used to define high quality data are often formulated in terms of rules rooted in the business processes that create or consume data. Stewards shall help the AfroCentric Group surface these rules in order to ensure that there is consensus about them and that they are used consistently.
13. **Managing data quality issues:** Stewards will be responsible for the identification and resolution of data related issues or in facilitating the process of resolution.
14. **Executing operational data governance activities:** Stewards are responsible for ensuring that, day-to-day and project-by-project, data governance policies and initiatives are adhered to. They should influence decisions to ensure that data is managed in ways that support the overall goals of the AfroCentric Group.

Business Data Owners must review each data they are responsible for and determine its overall impact level as follows:

- If it matches any of the predefined types of restricted information listed in Appendix A, the data owner assigns it an overall impact level of “High.”
- If it does not match any of the predefined types in Appendix A, the Business Data Owner should determine its information type and impact levels based on the guidance provided in Appendix B. The highest of the three impact levels is the overall impact level.
- If the information type and overall impact level still cannot be determined, the Business Data Owner must work with the Data Custodians to resolve the question.
- The Business Data Owner assigns each piece of Data a classification label based on the overall impact level:

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 28
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

- The Business Data Owner records the classification label and overall impact level for each piece of data in the official data classification table, either in a database or on paper.
- Data custodians apply appropriate security controls to protect each piece of data according to the classification label and overall impact level recorded in the official data classification table.
- Data Stewards apply information security controls to each piece of data according to its classification label and overall impact level.
- Original top secret and secret records must be kept for the purpose for which it was collected and thereafter should be transferred to Company Secretary for safe keeping.
- Only declassified records may be made available to the public through the PAIA request.

<i><b>Overall impact level</b></i>	<i><b>Classification label</b></i>
<i>High</i>	<i>Restricted/Sensitive Data</i>  <i>Secret / Classified Data</i>  <i>Special Personal Information</i>
<i>Moderate</i>	<i>Confidential Data</i>  <i>Personal Information</i>
<i>Low</i>	<i>Public</i>

### **PART VI - RETENTION OF DATA OF PERSONAL AND SPECIAL PERSONAL INFORMATION**

The Group shall not retain records of personal information and/or special personal information for longer than it is necessary for achieving the purposes for which the information was collected or subsequently processed unless:

- the retention of the record is required or authorised by law;
- the record is required by the Responsible Party for lawful purposes related to its functions or activities;
- the retention is required by a contract between parties; or
- the Data Subject or a competent person where the Data Subject is a child has consented to the retention of the records.

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 29
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

The purpose of this section of the Policy is to ensure that records of personal and special personal information:

- are adequately protected and maintained during retention;
- which are no longer required are destroyed, erased or discarded at the appropriate time.

All records of personal and special personal information that the Group has in its possession either as Responsible Party or Operator in the stead of its stakeholders, must be stored and archived in a place which can be accessed by more than a single person in the any one company of the Group. This is necessary to ensure that when one person is away from the office the other person is able to assist the Group during a Disaster Recovery Incident or Business Continuity situation.

Annexure A contains a guideline of the retention periods that the Group shall adhere to and observe. The purpose of Annexure A is to help the Group calculate appropriate retention periods at the outset of any processing activity.

Records of personal and special personal information may be retained in excess of the retention periods stated in Annexure A for historical, statistical and research purposes. The Group must ensure that there are appropriate safeguards against the inappropriate or unlawful use.

All personnel of the Group must ensure that the retained records of personal and special personal information contained in any format or record are only processed for the purpose that it is collected and that any new processing activities are promptly reported to the Group's Data Owners.

Data Owners shall ensure that they assist the Information Office with the identification of records which must be corrected, disposed of or archived. The principles of data protection contained in this Policy must be considered when making determination regarding, classification, retention, and disposal of records.

Employees who leave employment of the Group who had access to documents or data managed by them as per the scope of their employment, must ensure that such information is not held by them in isolation, this information should be available and accessible to the Group. Consequently, important company data including special personal information should be stored as follows:

1. By using the SharePoint Facilities;
2. By using the Document Facilities;
3. By using Department "sharepoints";
4. By using specific facilities such as the contract management system and ensuring that LGRC always has a copy of any contract that is managed by any Afrocentric Group schemes and business units.

This approach also ensures that the records of personal and special personal information are backed up as part of the regular back up procedures and where applicable the records of information can be made easily available in a Disaster Recovery or Business Continuity situation.

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 30
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

The affected Responsible parties has absolute rights to access all data that is maintained by an individual and AfroCentric Technologies can recover that data for whatever purpose whether that person is or is no longer in Group employment. Nevertheless, company information should ultimately be stored in a central place accessible by people who have rights to that data.

Company information and important documents and data should not be stored on the local drives of Desktops or Notebooks. These drives are not backed up and the disks can fail resulting in the data being lost. It is very expensive exercise to recover lost data using specialists in data recovery. Desktops and Notebooks have also been lost or stolen with the resultant loss of data stored on local drives.

All the Group websites contain web links to other websites. The Group will not share Personal Information with those websites but where a Data Subject decides to follow the link to such websites it is not the Group’s responsibility to maintain or establish appropriate privacy practices for such third party websites. We encourage all users to learn about the privacy policies of third party companies prior to following such links.

Should the user leave any of the Group’s website, whether through the utilisation of such a link or otherwise, the Group is not responsible for any harm which the user may suffer by accessing any information outside our website.

Website may contain links to websites operated by other companies. Some of these third party sites may be co-branded with the Group/ any Group subsidiary’s logo, even though they are not operated or maintained by the Group. Although business partners are carefully selected, we are not responsible for the privacy practices of websites operated by third parties that are linked to any Group company’s website. Once the user has left any Group company website, or any other digital channel maintained by us, the user must be aware of the applicable privacy policy of the third party website to determine how they handle the information they collect from the user.

### **B. Agents or service providers**

The Group may outsource the processing of certain functions and/or information to third parties. When we do outsource the processing of Personal and Special Personal Information to third parties or provide Personal and Special Personal Information to third-party service providers, we oblige those third parties to protect all personal information with the appropriate security measures in accordance with our standards and applicable law.

### **C. Business transfers**

The Group may engage with third parties to whom we may choose to sell, transfer, or merge parts of our business or our assets. Alternatively, we may seek to acquire other businesses or merge with them. If a change happens to our business, then the new owners may use the Personal and Special Personal Information collected by the Group in the same way as set out in this privacy notice.

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 31
Review Date:	31 August 2023	

#### **D. Legal requirements**

The Group reserves the right to disclose any Personal and Special Personal Information we have concerning any Data Subject if we are compelled to do so by a court of law, requested to do so by a governmental entity, or if we determine it is necessary or desirable to comply with the law or to protect or defend our rights or property in accordance with applicable laws.

We also reserve the right to retain Personal and Special Personal Information collected and to process such Personal and Special Personal Information to comply with accounting, tax rules, regulations and any specific record retention laws.

We require all employees and third parties to respect the security of all personal information and to treat it in accordance with the law. We do not allow our third-party service providers to use any Personal and Special Personal Information received from us for their own purposes and only permit them to process your personal information for specified purposes and in accordance with our instructions.

#### **E. Security of personal and special personal information**

Personal Information shall be treated as confidential and collected, processed and stored by the Group and our service providers in a manner that ensures appropriate security thereof, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures, which include:

- identity and access management;
- infrastructure and operations security;
- vulnerability management;
- business continuity planning;
- disaster recovery planning; and
- security awareness.

The Group continues to deal with any suspected data security breach and will notify all affected Data Subjects and any applicable regulator of a suspected breach where we are legally required to do so.

We will use all reasonable endeavours to ensure the integrity, security and confidentiality of all personal information submitted and/or obtained from a user, it will not be held liable under any circumstances if such information is compromised, disseminated or otherwise disclosed through conduct outside the control of the AfroCentric Group such as hacking, infection by “viruses”, “Trojan Horses” or any other computer programming routines or software that are intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data or personal information.

#### **F. Children and privacy**

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 32
Review Date:	31 August 2023	



## GROUP DATA PRIVACY POLICY

The Group digital platforms are not intended for use by children under the age of 14 years. The Group shall not knowingly solicit personal information from children under the age of 14 years or knowingly send requests for personal information.

Where a child dependent utilises the website, the mobile application or any other digital channel, and it is not apparent that the child is under the age of 14, then the AfroCentric Group will in good faith process, utilise, store and share the information unless otherwise notified, or it subsequently becomes apparent that the child is under the age of 14. The AfroCentric Group shall not have the obligation to verify the veracity of any information submitted to it.

### G. Breaches notification

Where there are reasonable grounds to believe that the Personal Information of a Data Subject has been accessed or acquired by any unauthorised person, the Responsible Party must notify the Information Regulator and the affected Data Subject, unless the identity of such Data Subject cannot be established.

The notification must be made immediately after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the Responsible Party's information system.

The Responsible Party may only delay notification of the Data Subject if a public body responsible for the prevention, detection or investigation of offenses or the Information Regulator determines that notification will impede a criminal investigation by the public body concerned and must be in writing and communicated to the Data Subject in a prescribed manner.

The notification must provide sufficient information to allow the Data Subject to take protective measures against the potential consequences of the compromise, including all of the following:

- A description of the possible consequences of the security compromise;
- A description of the measures that the responsible party intends to take or has taken to address the security compromise;
- A recommendation with regard to the measures to be taken by the Data Subject to mitigate the possible adverse effects of the security compromise; and
- If known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the Personal Information.

### PART IX - GROUP INFORMATION OFFICER

By default, the CEO of the Group will fulfil the role of Information Officer, but the responsibilities may also be delegated to any person duly authorised by the CEO of the Group. This delegation will be in the form of a formal appointment/delegation letter, where the roles and responsibilities of the Information Officer, are delegated to a suitable candidate within the Group.

Save for the draft guidelines on the registration of Information Officers, POPIA provides limited guidance to the qualifications and requirements for a person to be appointed as Information Officer, hence turning to the working party 29 guidelines on data protection officers.

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 33
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

The working party 29 guidelines prescribe that the Group must consider the following requirements when appointing a data protection officer:

- The appointed person must have expert knowledge of data protection law and practices.
- The person would typically be a privacy professional who has spent most of their career practicing privacy law.
- Consideration should be given to the Group’s unique requirements in light of the criteria expected of data protection officers.
- Considering the requirements above, the role of Information Officer will be delegated to the personnel in the Group’s Legal Governance Risk and Compliance division.

The Group’s Information Officer will have the following responsibilities:

- the encouragement of compliance with the Processing Conditions.
- dealing with requests made to the body pursuant to POPIA.
- working with the Information Regulator in relation to investigations conducted under POPIA.
- ensuring compliance with the provisions of POPIA.
- developing, implementing, monitoring and maintaining a compliance framework.
- conducting a personal information impact assessment to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.
- developing, monitoring, maintaining and making available a manual as prescribed in PAIA.
- developing internal measures together with adequate systems to process requests for information or access thereto.
- conducting internal awareness sessions regarding the provisions of POPIA, the regulations to POPIA, codes of conduct, or information obtained from the IR.

The Group’s Information Officer will take up his/her duties in terms of POPIA o after he or she is registered with the Information Regulator. The Information Officer may appoint (in writing) as many Deputy Information Officers as necessary. For example, the appointment of Deputy Information Officers may become necessary to make the organisations records as accessible as reasonably possible for requesters.

### **PART X - RESTRICTION OF PERSONAL AND SPECIAL PERSONAL INFORMATION**

**The Group shall restrict** processing of Personal and Special Personal Information if –

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 34
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

- the accuracy of such personal information is contested by the Data Subject, for a period enabling the Responsible Party to verify the accuracy of the information;
- the Responsible Party no longer needs the personal and special 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;
- the processing is unlawful and the Data Subject opposes its destruction or deletion and requests the restriction of its use instead; or
- the Data Subject requests to transmit the personal data into another automated processing system.

### **PART XI - PRIOR AUTHORISATION**

If necessary, and where there is no particular code of conduct by the Information Regulator in respect of any one business activity within the Group or in a specific sector of the business community, the Group shall request prior authorisation from the Information Regulator where it intends to process –

a) any unique identifiers of Data Subjects

- For a purpose other than the one for which the identifier was specifically intended at collection; and
- With the aim of linking the information together with information processed by other responsible parties.

A Unique Identifiers may be but are not limited to employee numbers, customer reference numbers assigned to transactions, membership numbers, and identity numbers.

Unique Identifiers must be distinguished from standard personal information such as names, surnames, addresses, and special personal information such as religious or philosophical beliefs, race or ethnic origin and sex life. Unique Identifier constitute something more than the aforementioned types of personal information.

Unique identifiers may also go further to include Internet Protocol addresses (“IP address“) which may not only serve to identify an individual but also disclose their location as well.

- b) process information on criminal behaviour or on unlawful or objectionable conduct on behalf of third parties;
- c) process information for the purposes of credit reporting;
- d) transfer special personal information, or the personal information of children, to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

### **9. POLICY REVIEW**

The policy will be reviewed after every two years but may be reviewed more frequently dependent on best practices, approaches and changes to the business or regulatory landscape in which this policy operates.

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 35
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

### 10. GRIEVANCE PROCEDURE

Any person who is not satisfied with the implementation of this policy shall follow the organisational grievance procedure.

### 11. RIGHT TO LODGE A COMPLAINT TO THE INFORMATION REGULATOR

Any person may submit a complaint to the Regulator alleging interference with the protection of the Personal Information.

Any queries relating to the lodging of a complaint should be directed to:

The Information Regulator (South Africa) 3 JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001 Website: [www.justice.gov.za](http://www.justice.gov.za) Email: [inforeg@justice.gov.za](mailto:inforeg@justice.gov.za)

### 12. MONITORING AND ENFORCEMENT

- All employees will be responsible for administering and overseeing the implementation of this policy including the supporting of guidelines, standard operating procedure, notices, consents and appropriate related documents and processes.
- Employees who violate the guidelines and standard operating procedures of this policy may be subjected to disciplinary action, being taken against him/her.
- The point of contact for requests, disclosures, questions, complaints and any other inquiries relating to the processing, collection, or re-identifying of personal information shall be directed to the Information Officer or the line manager.

### 13. POLICY APPROVAL



**GROUP CHIEF EXECUTIVE OFFICER**

20 September 2021

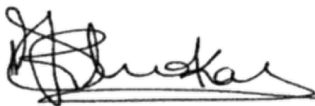
**DATE**



**GROUP CHIEF FINANCIAL OFFICER**

17 September 2021

**DATE**



**CHAIRPERSON:EXECUTIVE ERCO**

16 September 2021

**DATE**

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 36
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

### ANNEXURE A

#### RETENTION SCHEDULE

##### Minimum retention periods

**Column 1** lists the minimum periods of retention required for original or electronic records.

**Column 2** lists the minimum period of retention for the original record if an electronic copy is made.

**Column 3** lists the Act which refers to the period of retention, or if there is no relevant Act, the recommended standard practice (detailed references at the end of the Schedule).

Document	Minimum Period of Retention (in years)		
	Original / Electronic copy	Original if Electronic copy made	Reference
<b>Accounting Records</b>			
<i>Records to be kept by person who has rendered a return (from date return was lodged) including:</i>			
- Ledgers	15 (7)	3	11 & 24 (5)
- Cash books	15 (7)	3	11 & 24 (5)
- Journals	15 (7)	3	11 & 24 (7)
- Cheque books	7	3	5 & 11
- Bank statements	7	3	5 & 11
- Deposit slips	7	3	5 & 11
- Paid cheques	7	3	5 & 11
- Invoices	7	3	5 & 11
- Stock lists	15 (7)	3	11 & 24 (5)
- Other books of account	15 (7)	3	11 & 24 (5)
- Electronic representations of information	Indefinite (7)	Nil	11 & 24 (5)
<i>Records relating to taxable capital gain or assessed capital loss (from date return was lodged) including:</i>			
- Agreement for acquisition, disposal or lease of asset	5	1	11
- Details of asset transferred into a trust	5	1	11
- Copies of valuations used in determining the taxable capital gain or assessed capital loss	5	1	11
- Invoices or other evidence of payment records such as bank statements and paid cheques relating to any costs claimed in respect of the acquisition, improvement or disposal of any asset	5	1	11

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 37
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

Document	Minimum Period of Retention (in years)		
	Original / Electronic copy	Original if Electronic copy made	Reference
Annual financial statements, from the date on which they were issued	15 (7)	3	11 & 24 (5)
Annual financial statements working papers	5	1	11
Ancillary books of account and supporting schedules	15 (7)	3	11 & 24 (5)
Bank instructions	5	1	11
Bills of exchange	6	1	16
Consolidation schedules	15 (7)	3	11 & 24 (5)
Costing records	15 (7)	3	24 (5)
Creditors' invoices and statements	15 (7)	3	24 (5)
Creditors' ledgers	15 (7)	3	11 & 24 (5)
Debtors' ledgers	15 (7)	3	11 & 24 (5)
Debtors' statements	5	1	11
Dividend and interest payment lists (listed company)	15	3	5
Fixed asset register	15 (7)	3	11 & 24 (5)
Goods received notes	5	1	11
Insolvent businesses – record of transactions	3 years prior to sequestration	1	12
Insolvent estates (books and documentation in possession of trustee)	6 months after Master's confirmation of final trustee's account	6 months after Master's confirmation of final trustee's account	12
Payrolls	5	1	3, 6 & 11
Petty cash books	15 (7)	3	11 & 24 (5)
Purchase invoices (with supporting documentation)	5	1	11
Purchase journals (with supporting documentation)	15 (7)	3	11 & 24 (5)
Purchase orders	5	1	11
Railage and shipping documents	5	1	11
Receipts	5	1	11

Document	Minimum Period of Retention (in years)
----------	--

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 38
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

	Original / Electronic copy	Original if Electronic copy made	Reference
Sales invoices (with supporting documentation)	5	1	11
Year-end working papers for companies	5		11
<b>Company Records</b>			
Annual financial statements including: - Annual accounts - Directors' report - Auditor's report	15	3	24
Certificate of Incorporation	Indefinitely	3	24
Certificate of change of name (if any)	Indefinitely	3	24
Memorandum and Articles of Association	Indefinitely	3	24
Certificate to commence business (if any)	Indefinitely	3	24
Memorandum of Incorporation, as amended from time to time	Indefinitely	3	5
Rules of the company	Indefinitely	3	5
Record of current and past directors (for past directors, from date past director retired from company), including: - Full name and any former names - Identity number, or, if not, date of birth - Nationality and passport number, if not a South African - Occupation - Address for service - Date of last appointment as director - Name and registration number of every other company or foreign company of which the person is a director or prescribed officer - In the case of a company that is required to have an audit committee, the professional qualifications and previous experience of the director	7	3	5
Copies of all reports presented at an annual general meeting of the company, from the date of the meeting	7	3	5
Notices and minutes of all shareholders meetings, including: - All resolutions adopted by them - Any document that was made available by the company to the shareholders in connection with the resolution	7	3	5
Copies of all written communication sent to shareholders of different classes of securities after the date issued	7	3	5
Minutes of all meetings and resolutions of: - Directors - Directors' committees - Audit committee From the date of such meeting or on which such resolution was adopted	7	3	5
Minute books and resolutions passed at general / class meetings	Indefinitely	3	24

Document	Minimum Period of Retention (in years)
----------	--

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 39
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

	Original / Electronic copy	Original if Electronic copy made	Reference
Securities Register, including: - Uncertificated - the total number of securities that are held - Certificated - o Names and addresses of the people to whom the securities were issued o Number of securities issued to every person o The number of securities that have been placed in trust or whose transfer has been restricted o Securities other than shares – the number of the securities issued and outstanding or the names and addresses of the registered owners of a beneficial interest in the security	Indefinitely		5
Record of company secretaries and auditors, including name and date of appointment. In the case of a firm or juristic person, the name, registration number and registered address must be recorded	Indefinitely		5
Company's Registration Certificate	Indefinitely		5
Register of Allotments – after a person ceased to be a member	15	3	24
Branch register	15	3	24
Register of Members	15	3	24
Index of Members	15	3	24
Registers of mortgages and debentures and fixed assets	15	3	24
Register of Directors	Indefinitely	3	5
Register of Directors' shareholdings	15	3	24
Register of Directors and certain Officers	15	3	24
Directors' attendance register	15	3	24
Notification of change of address	1	Nil	1
Proxy forms: - Used	3	3	24
- Used at Court convened meetings	3	3	24
CM 25	Indefinitely	3	24
CM 26	Indefinitely	3	24
<b>Contracts and Agreements</b>			
Agreements of historical significance	Indefinitely	Nil	N/A
Debts – The Prescription Act should be referred to as the period depends on the type of debt	4 – 30		16
Indemnities and guarantees (after date of expiry)	5	Nil	1
Licensing agreements (after date of expiry)	5	Nil	1
Rental and hire purchase agreements, suspensive sale agreements (after date of expiry)	5	Nil	1
<b>Correspondence</b>			
General	3	Nil	1
Accounting related	5	Nil	1

Policy:	Group Data Privacy Policy		
Custodian:	Group Chief Financial Officer: Compliance		
Approval Date:	September 2021	Version No. 1.0	
Implementation Date:	September 2021	Page: 40	
Review Date:	31 August 2023		



## GROUP DATA PRIVACY POLICY

Document	Minimum Period of Retention (in years)		
	Original / Electronic copy	Original if Electronic copy made	Reference
Agreements (after termination)	5	Nil	1
<b>Electronic Data</b>			
Personal information	As long as needed or authorised by law	3	7 & 18
Record of personal information and the specific purpose for which it was collected (from when data is no longer used)	1	Nil	7
Record of third party to whom personal information was disclosed, as well as the date on which and the purpose for which it was disclosed (from when data is no longer used)	1	Nil	7
<b>Employee Records</b>			
Application for jobs – unsuccessful	1	Nil	1
Arbitration award records	3	Nil	13
Collective agreement records	3	Nil	13
Determination records made in respect of Wage Act	3	Nil	13
Disciplinary records for each employee, including: - Nature of any disciplinary transgressions - Actions taken by the employer - Reasons for such actions	Indefinitely	Nil	13
Prescribed details of any strike, lock-out or protest action involving employees	Indefinitely	3	13
Employment Equity Plan (from date of expiry of the plan)	3	1	8
Expense accounts	5	1	11
Payrolls	5	1	3, 6 & 11
Salary revision schedules	4	Nil	3 & 6
Salary wage register	5	1	6 & 11
Staff records (after employment ceases), including: - Employee's name and occupation - Time worked by each employee - Remuneration paid to each employee - Date of birth of any employee under 18 years of age - Amount of employees' tax deducted or withheld from the amounts of remuneration - Income tax reference number of employees registered as taxpayers - Skills Development Levy contributions - UIF contributions	3 3 3 3 5 5 5 5	Nil Nil 1 Nil 1 1 1	3 & 6 3 & 6 3,6, & 11 3 & 6 11 11 11 & 21 11 & 22
Tax returns – employees	5	1	11
Time and piecework records	4	Nil	3 & 6
Wage and salary records (including overtime details)	5	1	3, 6 & 11
Written particulars of employment (after termination of employment)	3	Nil	3

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 41
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

Document	Minimum Period of Retention (in years)		
	Original / Electronic copy	Original if Electronic copy made	Reference
<b>Financial Service Providers / Accountable Institutions</b>			
Premature cancellations of transactions or financial products by clients	5	Nil	9
Complaints received, together with an indication whether or not resolved	5	Nil	9
Compliance with fit and proper requirements	5	Nil	9
Cases of non-compliance with the FAIS Act and reasons therefore	5	Nil	9
Continued compliance by representatives with the requirements regarding their appointment and competence to act	5	Nil	9
Records of telephonic or electronic instructions received from clients (after termination of the product concerned or rendering of the financial service concerned)	5	Nil	9
Records of financial products owned by each client (after termination of financial products concerned)	5	Nil	9
Record of advice (after termination of the product concerned or rendering of the financial service concerned), including: <ul style="list-style-type: none"> <li>- Summary of data obtained from client</li> <li>- Products considered</li> <li>- Products recommended</li> <li>- Why they will satisfy client's needs and objectives</li> </ul>	5	Nil	9
Business relationships (from the date on which relationship terminates) and transactions (from the date of conclusion of the transaction), including: <ul style="list-style-type: none"> <li>- Identity of clients</li> <li>- If the client is acting on behalf of another person, the identity of the person on whose behalf the client is acting and the client's authority to act on behalf of that other person</li> <li>- If another person is acting on behalf of the client, the identity of that other person and that other person's authority to act on behalf of the client</li> <li>- Manner in which the identities of the abovementioned persons were established</li> <li>- Nature of that business relationship or transaction</li> <li>- In the case of a transaction, the amount involved and the parties to the transaction</li> <li>- All accounts that are involved in transactions</li> <li>- Name of the person who obtained the above data on behalf of the accountable institution</li> <li>- Any document or copy thereof obtained in order to verify a person's identity</li> </ul>	5 5 5 5 5 5 5 5	Nil Nil Nil Nil Nil Nil Nil Nil	10 10 10 10 10 10 10 10
<b>General</b>			
Audit working papers	5		2
Employment Equity Plan (from expiry of the plan)	3	1	8

Policy:	Group Data Privacy Policy		
Custodian:	Group Chief Financial Officer: Compliance		
Approval Date:	September 2021	Version No. 1.0	
Implementation Date:	September 2021	Page: 42	
Review Date:	31 August 2023		

## GROUP DATA PRIVACY POLICY

Document	Minimum Period of Retention (in years)		
	Original / Electronic copy	Original if Electronic copy made	Reference
<b>Health and Safety</b>			
Accident books and records	3	Nil	15
Health and safety committee recommendations to employers	3	Nil	15
Records of incidents reported at work	3	Nil	15
<b>Insurance Records</b>			
Claim reports and accident reports (after date of settlement)	3	Nil	1
Policies (after date of lapse)	5	Nil	11
<b>Investment Records</b>			
Certificates and other documents of title	Permanently or until sold	Nil	N/A
Schedules and documents (after date investment sold)	15 (7)	3	11 & 24 (5)
Share investment certificates	Permanently or until sold	Nil	N/A
Transfer of marketable securities	5	3	5, 11 & 24
<b>Medical Scheme Records</b>			
Assets – documents of title relating to assets held by a medical scheme or on behalf of a medical scheme	Permanently or until sold		14
Application forms for membership (from date of termination of membership)	7	3	1
Beneficiaries – members of medical schemes and their dependants	7	3	5, 11 & 14
Books of accounts for medical schemes under administration	7	3	5, 11 & 14
Claims – record of money paid out in respect of claims made by members in term of the benefits to which they are entitled under the scheme rules and the law	7	3	5, 11 & 14
Contributions from medical scheme members – amount and frequency	7	3	5, 11 & 14
Health service providers to whom claims payments have been made	7	3	5, 11 & 14
Minutes of resolutions of the board of trustees	7	3	5, 11 & 14
Operational records of medical schemes (scheme activities)	7	3	5, 11 & 14
<b>Pension Records</b>			
Actuarial valuation reports	10	Nil	1
Contribution records	5	1	11
Group health, life and personal accident policies (after date of final cessation of any benefit payable under the policy)	5	Nil	1
Individual life policies under “Top Hat” schemes (after date of final cessation of benefit)	5	Nil	1
Investment records	15 (7)	3	24 (5)

Policy:	Group Data Privacy Policy		
Custodian:	Group Chief Financial Officer: Compliance		
Approval Date:	September 2021	Version No. 1.0	
Implementation Date:	September 2021	Page: 43	
Review Date:	31 August 2023		

## GROUP DATA PRIVACY POLICY

Document	Minimum Period of Retention (in years)		
	Original / Electronic copy	Original if Electronic copy made	Reference
<b>Property Records</b>			
Deeds of title	Permanently or until disposed of	Nil	1
Leases (after date of expiry of lease and all queries have been settled)	5	Nil	1
Sectional title records	Permanently or until disposed of	Nil	1
Transfer duty records	Permanently or until disposed of	Nil	1
<b>RICA</b>			
Employer must record the following data before handing over a SIM-card to an employee: - Date and period for which the SIM-card is provided - Mobile Subscriber Integrated Service Digital Network number (MSISDN-number) of the SIM-card - Full names and surname, identity number and at least one address (residential, business or community based) of the employee concerned - Nationality and passport number of not a South African	5	1	19
<b>Share Registration Records</b>			
Acceptance forms	12	Nil	1
Allotment letters	15	3	24
Annual return and supporting documents	15	3	24
Application forms	12	Nil	1
Cancelled share or debenture certificates and balance receipts (many large transfer offices keep for one year only)	3	Nil	1
Cancelled share transfer forms	12	Nil	1
Change of address – notification	1	Nil	1
Dividends and interest: - Mandates (from date of receipt) - Paid warrants - Payment lists - Unclaimed	3 12 15 Until cleared or forfeited whichever is earlier	Nil Nil 3	1 1 1
Letters of indemnity for lost share certificates	Permanently	Nil	1
Power of attorney, stop notices and similar court orders (from date person ceased to be a member)	15	Nil	1

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 44
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

Document	Minimum Period of Retention (in years)		
	Original / Electronic copy	Original if Electronic copy made	Reference
Redemption / conversion discharge forms of endorsed certificates	12	Nil	1
Transfer records	5	1	20
<b>Tax Records</b>			
Income tax required records	5	1	11
Taxation returns and assessments	5	1	11
<b>VAT Documentation</b>			
Bank statements, deposit slips, stock lists, and paid cheques	5 years from date of last entry	1	23
Books of accounts	5 years from date of last entry	1	23
Details records of the registered vendors' transactions – all goods and services	5	1	23
Invoices, tax invoices, credit and debit notes	5 years from date of last entry	1	23
Systems documentation: - Charts and codes of accounts - Accounting system instruction manuals - Systems and programme documentation describing the accounting system used in each tax period in the supply of goods and services	5	1	23

### References for Column 3

1. Standard Practice
2. Auditing Profession Act, 26 of 2005 – *This Act implicitly requires that documents should be retained for 3 years.*
3. Basic Conditions of Employment Act, 75 of 1997; General Administrative Regulations
4. Civil Proceedings Evidence Act, 25 of 1965 – *In terms of this Act, a Court may, notwithstanding that an original document is not produced, in lieu thereof accept a copy of the original document or of the material part thereof proved to be a true copy.*
5. Companies Act, 71 of 2008 and Regulations, 2011
6. Compensation for Occupational Injuries and Diseases Act, 130 of 1993
7. Electronic Communications and Transactions Act, 25 of 2002 – *Section 15 of this Act governs the admissibility, evidential weight and procedure for submitting electronic evidence generated "in the ordinary course of business".*
8. Employment Equity Act, 55 of 1998; General Administrative Regulations, 2009
9. Financial Advisory and Intermediary Services Act, 37 of 2002; FAIS Codes of Conduct for Administrative and Discretionary FSPs, 2003; FAIS – General Code of Conduct for Authorised Financial Services Providers and Representatives, 2003
10. Financial Intelligence Centre Act, 38 of 2001; Money-Laundering and Terrorist Financing Control Regulations, 2002
11. Income Tax Act, 58 of 1962
12. Insolvency Act, 24 of 1936
13. Labour Relations Act, 66 of 1995
14. Medical Schemes Act, 131 of 1998 and Regulations

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 45
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

15. Occupational Health and Safety Act, 85 of 1993; General Administrative Regulations, 2003
16. Prescription Act, 68 of 1969 – *Prescription periods for various types of debts:*
  - Secured by mortgage bond – 30 years
  - Judgment debt – 30 years
  - In respect of any taxation imposed or levied by or under any law – 30 years
  - Owed to the State in respect of any share of the profits, royalties or any similar consideration payable in respect of the right to mine minerals or other substances – 30 years
  - Owed to the State and arising out of an advance or loan of money or a sale or lease of land by the State to the debtor – 15 years
  - Arising from a bill of exchange or other negotiable instrument or from a notarial contract – 6 years
  - Other – 3 years
17. Promotion of Access to Information Act, 2 of 2000
18. Protection of Personal Information Act, 4 of 2013
19. Regulation of Interception of Communications and Provision of Communication-related Information Act, 70 of 2002
20. Securities Transfer Tax Administration Act, 26 of 2007
21. Skills Development Levies Act, 9 of 1999
22. Unemployment Insurance Contributions Act, 4 of 2002
23. Value Added Tax Act, 89 of 1991
24. Companies Act, 61 of 1973; Regulations for the Retention and Preservation of Company Records, 1983

### RELEVANT LEGISLATION FOR DATA RETENTION

- Auditing Profession Act, 26 of 2005
  - Banks Act, 1990
  - Basic Conditions of Employment Act 75 of 1997
  - Children’s Act, 71 of 2005
  - Companies Act, 2008
  - Compensation for Occupational Injuries and Diseases Act, 130 of 1993
  - Constitution of the Republic of South Africa, 1996
  - Consumer Protection Act, 68 of 2008 (CPA)
  - Co-operatives Amendment Act, 6 of 2013
  - Electronic Communications and Transactions Act, 2002 (ECT)
  - Crimes and Cybersecurity Bill (not yet enacted)
  - Financial Advisory and Intermediary Services Act, 2002 (FAIS)
  - Employment Equity Act 55 of 1998
  - Financial Intelligence Centre Act, 2001 (FICA)
  - Health Professions Act, 1974
  - Income Tax Act, 58 of 1962
  - King IV Report on Corporate Governance and the King IV Code, 2017 (King IV Code™)
- 
- Labour Relations Act, 66 of 1995 (LRA)
  - Medical Schemes Act, 131 of 1998 (MSA)
  - Mental Health Care Act, 2002
  - National Credit Agreements, 34 of 2005
  - National Health Act, 2003
  - Occupational Health and Safety Act, 85 of 1993 (OHS)

Policy:	Group Data Privacy Policy	
Custodian:	Group Chief Financial Officer: Compliance	
Approval Date:	September 2021	Version No. 1.0
Implementation Date:	September 2021	Page: 46
Review Date:	31 August 2023	

## GROUP DATA PRIVACY POLICY

- Pension Funds Act, 1956
- Pharmacy Act, 1974
- Promotion of Access to Information Act, 2000 (PAIA)
- Protection of Personal Information Act, 2013 (POPIA)
- Regulation of Interception of Communications and Provision of Communication Related Information Act, 2002 (RICA)
- Tax Administration Act, 28 of 2011
- Unemployment Insurance Act, 63 of 2001
- Value Added Tax Act, 89 of 1991

This list is not exhaustive of all legislation which relates to retention of data, as other laws, regulations and standards may also be relevant.

**Acknowledgements:**

*Metrofile / Deloitte & Touche Guide on the Retention of Documents – 7<sup>th</sup> Edition 2003*

*SAICA Guide on the Retention of Records – May 2021*

### General Data Retention Provisions

Record type	Data storage mechanism	Minimum retention period	Maximum retention period
<b>Paper based original record</b> – no scanned copy	External records management company / Bulk filers / On-site storage	7 years	7 years
<b>Paper based original record</b> – scanned copy using standard scanning methods and policy of the Group	External records management company / Bulk filers / On-site storage	1 month	6 months
<b>Paper based original record</b> – scanned copy, specifically membership application forms	External records management company / Bulk filers / On-site storage	3 years after membership of that scheme ends	7 years after scheme membership ends
<b>Electronic record</b> – archived records	Archived tape storage	Purpose served – archived to “offline media” after 3 years	4 years from end of purpose having been served
<b>Electronic record</b> – “live” records	Centralised storage – short term retrieval	3 years after the purpose has been served	7 years
<b>Electronic record</b> – voice recordings and associated metadata	Centralised storage	3 years after the purpose has been served	7 years

Policy:	Group Data Privacy Policy		
Custodian:	Group Chief Financial Officer: Compliance		
Approval Date:	September 2021	Version No. 1.0	
Implementation Date:	September 2021	Page: 47	
Review Date:	31 August 2023		