THE AURUM INSTITUTE NPC

DATA PRIVACY POLICY

Policy Information

Policy Status: Approved

Maintained by: Data Management

The signatures below certify that this document has been reviewed, accepted, and demonstrates that the signatories are aware of all the requirements contained herein and are committed to ensure their provision.

Prepared by	Name	Marlize Pistorius	Signature and Date	Signed by:Marlize Pistorius Signed at:2024-10-02 10:01:15 +02:00 Reason:Witnessing Marlize Pistorius Marlize Pistorius
	Role	Technical Director		
Reviewed by	Name	Jacqueline Paterson	Signature and Date	Signed by:Jackie Paterson Signed at:2024-10-02 10:04:00 +02:00 Reason:Witnessing Jackie Paterson Paterson
	Role	Regional Director: Strategic Information, Data Operations		
Approved by	Name	Dave Clark	Signature and Date	Signed by:Dr Dave Clark Signed at:2024-10-03 12:02:09 +02:00 Reason:I approve this document Dr Dave Clark
	Role	Group COO		

Company Documents once printed are considered uncontrolled documents. Only documents in the Aurum Policy Centre online Library are the most current version.

TABLE OF CONTENTS

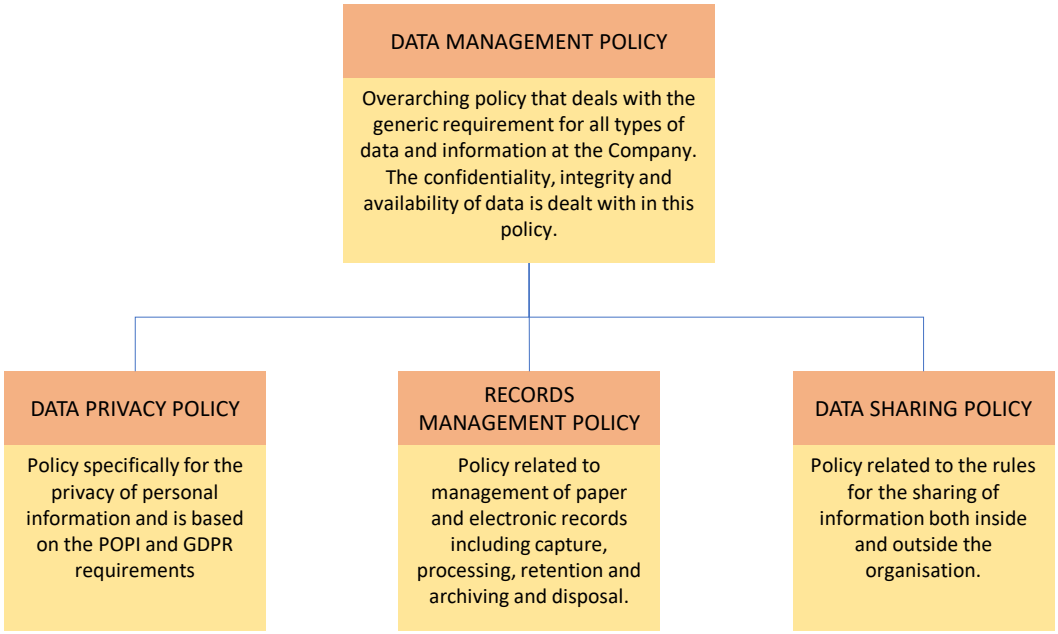
DATA PRIVACY POLICY

INTRODUCTION

1. Data is the lifeblood of any organisation. All transactions and management decisions are based on data. Organisations typically hold vast amounts of data. Much of this is confidential and organisations often may not be able to function in the absence of this data. It is crucial to correctly manage the integrity, availability, and confidentiality of data. With the onset of current global data privacy legislation, data privacy protection is a critical requirement that needs to be met by all organisations operating globally.

2. This policy is one of four (4) policies that deals with various aspects of data and information management at the Group (see Figure 1 below)

Figure 1: Data and Information Management Policies



SCOPE

3. This policy is relevant to the Aurum Institute NPC (the Group), including operations outside of South Africa, including Subsidiaries and Associate/Affiliate companies of the Group.

IMPLEMENTATION OF THE POLICY

4. Related policies, if any exist, that were in force prior to the commencement of this policy are replaced with effect from the date on which an Executive Director approves this policy.

5. This policy applies to all personal data collected, processed, or stored at the Group, whether on paper or electronic. This policy does not apply to personal data that is outside the control of the Group, even if the Group has access to this data.

PURPOSE OF THE POLICY

6. The purpose of this policy is to detail the mandatory data privacy requirements for the management of all personal information created, stored or processed at the Group.

DEFINITIONS AND ABBREVIATIONS

Definitions

7. **Classification** - Is the process of devising and applying schemes to the organisation of data or information based on the business activities that generate records, whereby they are categorised in systematic and consistent ways to facilitate their capture, retrieval, maintenance, and disposal.

8. **Controller** - This is the natural or legal person or persons, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The Group is the data controller for any data under the control of the Group.

9. **Data** - Data is raw, unorganised facts that need to be processed. Data can be found in databases, data sets, documents, instant messages, project plans, E-mails, etc. The form in which data is stored could be paper or electronic.

10. **Data Subject** - The person to whom the personal information relates to.

11. **De-identified Data** - This is personal data where all personal content has been removed or masked such that it is not possible to recover the personal content.

12. **Disposal** - Process associated with the implementation of decisions and processes for the deletion or destruction of records.

13. **Documents** - Are sets of recorded information that have not or not yet been assigned corporate value (for example drafts, meeting notes, staff holiday schedules etc.) because they do not need to be kept for legal or regulatory reasons and only have operational value for the organisation.

14. **Electronic records** - Information that is generated and stored electronically.

15. **General Data Protection Regulation** - The General Data Protection Regulation is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. It also addresses the transfer of personal data outside the EU and EEA areas.

16. **HIPAA**: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a USA federal law that resulted in a national standard to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The Privacy Rule standards address the use and disclosure of individuals' health information (known as protected health information or PHI) by entities subject to the Privacy Rule. HIPAA is specific to health information and is less strict than GDPR (General Data Protection Regulation), which applies to all personal information.

17. **Information** - Information is data that has been processed, organised, structured, or presented in each context to make it more useful.

18. **Opt-In**: Opt-in means that the person needs to take affirmative action to opt into use and processing of their data. Unless the person takes conscious action to indicate their approval, then processing may not take place.

19. **Opt-Out**: Opt-out means that processing of data will take place unless the user takes conscious action to indicate their rejection of the processing.

20. **Personal Data / Information** - Personal information is information such as contact details, age, race, birth date, and educational, medical, criminal, financial, and employment background.

21. **POPIA** – Protection of Personal Information Act

22. **Processor** - This is the natural or legal person or persons, public authority, agency, or other body which processes personal data on behalf of the controller. The Group could be the data *processor* for itself, a funder, the Department of Health, or a partner. Any other entity that processes the Aurum Group's information would also be a *processor*.

23. **Profiling** - This is any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

24. **Regulatory Authority** - This is the body in a particular jurisdiction that creates guidelines and regulations, monitors, investigates and enforces the privacy legislation and can allow or disallow exceptions.

25. **Special Categories of Personal Data / Sensitive Personal Information** - This consists of data revealing racial or ethnic origins, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Abbreviations

DAMA	Data Management Association
DMBOK	Data Management Body of Knowledge 2nd Edition
EEA	European Economic Area
EU	European Union
GDPR	General Data Protection Regulation
I&T	Information and Technology
ISO	International Organisation for Standardisation
PII	Personal Identifiable Information
POPIA	Protection of Personal Information Act

POLICY STATEMENT

26. This policy deals with the privacy of any personal information collected or held at the Group environment whether paper or in electronic form.

27. Any organisation that has access to or processes personal information held by the Group or on behalf of the Group is also subject to this policy.

POLICY CONTENT

28. Much of the data that is collected and used by the Group contains personal information. Personal information is tightly regulated by POPIA and other data protection standards. There are also significant penalties for non-adherence as well as the strong possibility of reputational risk. This policy states the minimum requirements to be met for the handling of personal information. If any other regulation, contract, or agreement stipulates more stringent requirements, then those more stringent requirements will apply to the data in respect to which such refers.

29. For the purposes of this policy all usage of the term information includes data and usage of the term data includes information.

General

30. **Data Governance Forum:** The Data Governance Forum (as defined in the Data Management Policy) oversees the implementation of the data privacy requirements.

Data Privacy and Confidentiality

31. **Data Collection Scope**: The Group must ensure that only data that is required for business purposes is collected from external parties. This applies especially to personal information about natural persons. [POPI][GDPR-A5]. The design of systems must be such that only the necessary information is collected [GDPR-A25]. The collection of more sensitive type of personal information (Special Categories of personal information as defined in Definitions Section) is only allowed under exceptional conditions. [GDPR-A9]

32. **Direct Collection**: Personal information must be collected directly from the data subject. [POPIA]. For any information not directly collected, the data subject must be informed of this data collection and processing. The following information must be provided to the data subject when the personal data is collected and when an enquiry is made by the data subject [GDPR-A13] [GDPR-A14]:

    32.1. Identity and contact details of responsible person at the Group.

    32.2. The purpose and legal basis for the processing.

    32.3. The legitimate interest pursued by the controller with the processing of this data.

    32.4. The recipients or categories of recipients of the personal data, if the information is transferred outside the Group or outside the country of origin.

    32.5. Whether the personal data is to be transferred to another country.

    32.6. Where the data is collected from a separate person rather than directly from the data subject, the data subject must be informed of what data has been collected.

33. **Consent**: The Group must obtain consent for the collection and specific use of data from the data subject. This consent must be clear and transparent. For personal information of a child under the age of 16, the consent of the parent or legal guardian is required. Consent may only be via Opt-In, not Opt-Out. This consent needs to be stored in a secure manner where the consent can be retrieved if required. [GDPR-A7]

34. **Withdrawal of Consent**: Consent given by a data subject may be withdrawn at any time and the data subject needs to be informed of their right to withdraw consent. Simple-to-use facilities to enable the withdrawal of consent must be provided. [GDPR-A8]

35. **Data Processing**: Any processing of personal data must be lawful and as set out in the consent. [GDPR] Only additional processing that is compatible with the original use is allowed without additional consent being obtained. No other use of the data is allowed unless a new consent is obtained for such use. [GDPR-A6] [POPIA]. NO personal information may be shared on any platform, without additional security measures. Images containing personal information must be redacted to ensure no PI is shared. Documents containing personal information must be classified as such and comply with Department of Health policies and procedures if it is necessary that they be shared for operational purposes.

36. **Query Personal Information**: A data subject, whether the Group stores or does not store their personal information, has a right to query whether the Group stores their personal information. The Group must be able to respond quickly to any request from any natural person regarding any personal information relating to that person it has or does not have in its possession. [GDPR-A15]

37. **Data Erasure**: The data subject can request that the personal data requested be erased, in which case, the data needs to be erased or de-identified unless a legitimate reason for not deleting the data or de-identifying the data exists [GDPR], typically for organisational records or to service the data subject. The Group must ensure that the personal information is either de-identified or destroyed when the information is no longer needed. [POPIA] [GDPR-A17]. For

research projects, this will be dependent on the requirements of the research project as specified by the funder. Data on existing backups does not need to be erased as this could compromise the integrity of all other data in these backups.

38. **De-Identified Data**: Data that has been de-identified does not need to comply with the privacy requirements in this policy as the person involved cannot be determined. However, this does not absolve Group users or processors from the obligation to protect and secure data.

39. **Data Accuracy**: The Group must attempt to ensure that the data is accurate by means of process or system design. The accuracy of the data must be checked whenever the Group contacts the data subject. If the data subject informs the Group of any inaccuracy in the data, this must be corrected. [GDPR-A5] [POPIA]

40. **Data Portability**: The Group must be able to extract personal information for any specific data subject and provide this in a manner suitable for transfer to the data subject or another controller. This must be in the form of a structured, commonly used, and machine-readable format. This only applies to data that is under the control of the Group. [GDPR-A20]

41. **Data Integrity and Confidentiality:** Measures must be taken to ensure the integrity of the personal information and to prevent loss, damage, or unlawful access to the information. It is required that the internal and external risks be identified, and safeguards be put into place to mitigate these risks. These safeguards must be tested and updated as and when necessary.

42. **3rd Party Privacy Adherence**: If any of the data capturing or processing is outsourced to 3rd parties, then the Group must ensure that the 3rd party meets the data privacy requirements in this policy [POPIA] [GDPR-A28] [GDPR-A32]

43. **Data Breach Procedures**: The data subject must be informed of any breach involving their information as soon as possible after the breach has taken place. The relevant regulatory authority and funder/(s) must also be informed of such a breach if the scope of the data collected falls within their jurisdiction. [GDPR-A33] [GDPR-A34] [POPIA].

44. **Data Leakage Protection and Detection:** Procedures and automated tools must be implemented to ensure that confidential information is not accidently or deliberately released into the public domain or to unauthorised persons within or outside the Group. Procedures need to be put into place to detect any data leakage that takes place. [NIST AC-22] [NIST IR-9]

45. **Data Sovereignty**: Personal data must be stored in the country where the person resides or where the data was collected. If this is not possible, then the data must be stored only in a country where the privacy laws are compatible with the country in which the data was collected.

46. **Data Transfer**: The transfer of data out of that country is possible for processing, but the data subject must be informed of this transfer. The processor (and country) needs to meet the GDPR or POPIA requirements, the relevant country legislation and regulations, and any funders specific requirements. [GDPR-A44] The conditions under which the transfer of data is possible includes; the country has already been deemed to offer adequate levels of data privacy protection that is equivalent to or exceeds those of the source country or that the controller and/or processor have offered safeguards, and the data privacy laws protect data subjects' rights and are enforceable. [GDPR-A45] [GDPR-A46] [NIST AC-21]

47. **Automated Processing**: The data subject has a right to not be subjected to decisions made purely by automated means. This includes profiling. [GDPR-A22]

48. **Complaints Procedure**: An accessible complaints procedure must be set up and made publicly available. The data subject needs to be made clearly aware of the existence of the objection and complaints process and procedures. [POPI][GDPR-21]

49. **Data Privacy Notices**: Notification of the data subject's rights and remedies must be included in all customer-facing documents or any interfaces in which the data subject enters their

personal information. [GDPR-A12]

50. **Demonstrable Compliance**: The Group must implement appropriate technical and process measures to ensure and demonstrate that the processing of personal information is performed in accordance with GDPR and POPI (where applicable). [GDPR-A24]. A record of all processing of personal information, whether insourced or outsourced, must be kept. [GDPR-A30]

51. **Prior Consultation for High-Risk Scenarios**: For data privacy processing that is deemed to be considerable risk (places the funders' provided system does not meet expected information security and confidentiality standards), there must be consultation with the ethics committee, funders, and/or regulatory authority before processing starts. [GDPR-A36]

CONTRAVENTIONS

52. As contravention of this Policy is a serious matter, it may result in disciplinary action taken in terms of the country Disciplinary Code as promulgated.

COMPLIANCE REQUIREMENT

Obligations	Source	Compliance Risk Category
☒ International/ National Standards:	ISO 27000: Information Security Best Practices DAMA DMBOK Second Edition Regulation (EU) 2016/679 (General Data Protection Regulation of 2018)	Reputational Impact
☒ Statute/s:	South African Protection of Personal Information Act No. 4 of 2013 (as amended) and King IV Report on Corporate Governance for South Africa, 2016 Primary legislation in Ghana, Data Protection Act, 2012 (Act 843) In Mozambique there is no specific legislation on data protection or privacy. However, the following sources of law impose some privacy obligations: 1. The Civil Code (Decree-Law no. 47344, of November 25, 1966, in force in Mozambique through Edict no. 22869, dated September 4, 1967) 2. The Penal Code (Law n0. 35/2014 of December 31) 3. The Labour Law (Law no. 23/2007, of August 1) 4. The Electronic Transactions Law (Law no. 3/2017, of January 9)	Legal Impact
☐ Regulation/s:		Not Applicable
☒ Internal Policy Standards:	POL DM 001, Data Management, Annexure A POL DM 002, Data Privacy Policy POL DM 004, Records Management Policy POL ICT 001, IT Security Policy	Business Impact

Obligations	Source	Compliance Risk Category
	POL ICT 002, End User Policy	
☐ References		Not Applicable

REVISION HISTORY

Amendment Record

This document is reviewed to ensure its continuing relevance to the systems and process that it describes. A record of contextual changes, additions or omissions is given below.

Ver #	Approval date	Next Review date	Context	
			Page No.	Significant Changes
1	01/12/2020	12/2022	1-7	First authorised version
2	10 May 2023	May 2025	1-7 6-7 7	Review dates and version control adjusted. Compliance Requirements added. Clauses related to implementation of controls moved to Data Management Policy.
3	1 November 2023	November 2025	1-8	Minor grammatical errors corrected and dates aligned.
4	14 October 2024	October 2026	5	Point 35. Detail added on sharing of personal information